Après la panne : Oxalide s'explique

En pleine campagne OpFrance de défacement de sites français, Oxalide, hébergeur de nombreux sites de presse français (*L'Express, Le Parisien, 20 Minutes, France Inter, Mediapart, Marianne, Slate.fr*...), a connu une indisponibilité d'environ 2 heures. Une panne et non une attaque contre la presse hexagonale, a depuis expliqué la société.

Son directeur associé, **Maxime Kurkdjian**, revient pour Silicon.fr sur les origines de ce dysfonctionnement causé par un Broadcast Storm (littéralement tempête de diffusion se caractérisant par des trames tournant indéfiniment sur le réseau et consommant une bonne partie des ressources) et sur les contre-mesures que va prendre l'hébergeur pour éviter que ce type d'incident ne se reproduise.

Silicon.fr : que s'est-il passé précisément ce vendredi 16 janvier au matin ?

Maxime Kurkdjian : L'élément déclencheur peut paraitre anodin : il s'agit d'une boucle réseau qui s'est créée sur le réseau d'administration, autrement dit une incompatibilité entre le brassage logique et le brassage physique. Concrètement, tout part d'équipements qui ont été connectés sur un switch d'administration jeudi 15, sur notre site PA3 (un des trois datacenters d'Oxalide, NDLR). C'est une erreur dans la documentation qui a abouti à cette manipulation impropre. L'allumage de ces équipements, vendredi matin, a déclenché la boucle réseau. Derrière, un enchaînement de circonstances a amené la panne qu'on a connue.

Dans cet enchaînement de circonstances, le contexte, et notamment la vague d'attaques contre des sites français, a-t-il joué un rôle ?

OpFrance a assurément joué un rôle dans le diagnostic. Du fait du contexte, on a d'abord commencé par regarder vers l'extérieur, pensant à une attaque. Mais d'autres éléments ont aussi joué un rôle clef. D'abord, les choix de design de notre réseau d'administration ont facilité la propagation du Broadcast Storm sur l'ensemble des datacenters. Ensuite, nos équipements cœur de réseau Juniper ont très mal réagi à la boucle qui s'était créée sur le réseau d'administration. Quatre d'entre eux sont tombés en même temps du fait du trafic sur leurs interfaces de management. Après échange avec le constructeur, il s'avère que ces dernières ne sont pas protégées des Broadcast Storm.

Etes-vous certain qu'il s'agisse d'une panne ? Un Broadcast Storm peut aussi être causée par un assaillant...

Nous avons reproduit l'incident deux fois dans la nuit de vendredi à samedi pour nous en assurer. C'est d'ailleurs comme cela que nous sommes remontés au switch à l'origine de la panne. Cette nuit-là, nous avons remonté le réseau d'administration machine par machine, pour découvrir l'équipement en cause, une baie sur laquelle nous étions en train d'intégrer de nouveaux clients.

Vendredi matin, l'urgence était de remettre les services en marche. Nous avons donc utilisé des mesures de contournement, en décommissionant le réseau d'administration. Nous n'avions alors plus de monitoring. Ce n'est que dans la nuit que nous avons démarré la phase de diagnostic, car celle-ci comportait un risque.

Quelles mesures allez-vous prendre pour éviter qu'un incident de ce type ne se reproduise ?

La 'to do list' est déjà assez longue. D'abord, nous allons décommissionner notre réseau d'administration, aujourd'hui commun à l'ensemble de nos datacenters, pour en créer 9 différents, chacun étant dédié à un site et à un niveau de criticité. Trois niveaux ont été définis sur chacun de nos trois sites. Cela sera fait courant février et empêchera qu'un événement de ce type ne se reproduise. Ensuite, nous allons remodeler nos moyens d'accès. Nous disposions d'un accès par Freebox, mais qui n'a pas fonctionné le jour de la panne car le switch nous reliant à l'équipement Opengear était lui aussi touché par le Broadcast Storm. Cette liaison va être modifiée, en utilisant du câble croisé. Concernant nos accès d'administration, une fibre noire arrivera directement sur les équipements dédiés.

Concernant la documentation, notre projet de CMDB (Configuration Management DataBase ou base de données de gestion de configuration, NDLR) doit être mené à son terme en 2015, en parallèle du déploiement d'un protocole d'audit de réseau qui nous permettra de comparer ce qui est répertorié avec ce qui est réellement en production.

Enfin, tout un volet concerne la lutte contre les Broadcast Storm, contre lesquelles existent des mécanismes de protection. Mais nous voulons tester ces automatismes car nos clients de la presse connaissent des trafics très fluctuants. Il ne faudrait donc pas que ces mécanismes les impactent. Nous allons également mettre à jour nos routeurs cœur de réseau : car au-delà de la version 12, Junos (l'OS de Juniper, NDLR) n'est plus sensible au trafic sur les interfaces de management.

Vos SLA ont-ils été dépassés lors de cet incident ?

Oui, et cela ne nous était plus arrivé depuis janvier 2010. Nous disposons d'un délai d'une heure pour le rétablissement de service. Or, ce vendredi 16 janvier, selon les sites, l'indisponibilité a varié entre 90 minutes et un peu plus de 2 heures.

Cette panne a mis en évidence le rôle central d'Oxalide auprès de la presse française. Etes-vous de ce fait devenu une cible ?

Nous connaissons les attaques DDoS (par déni de service, NDLR) depuis un certain nombre d'années. Nous cloisonnons beaucoup les environnements de nos différents clients pour les contrer. L'été dernier, « l'hacktiviste » Ulcan a ainsi visé Mediapart, un de nos clients. Mais, jusqu'à présent, ce n'est pas Oxalide qui était visé. La panne qui ne nous avons connue nous a rendu plus visible. Nous sommes devenus une proie intéressante. La semaine dernière, les attaques DDoS nous ciblant ont atteint un niveau important, dépassant les limites de nos mécanismes de protection automatique. Une intervention manuelle a donc été nécessaire pour lutter contre certaines attaques. Même s'il est impossible d'affirmer que cet épisode soit lié à la panne et à notre exposition médiatique, notre niveau de vigilance a été relevé.

A lire aussi :

Indisponibilité d'Oxalide : une erreur humaine et non une attaque
Défaillance d'Oxalide : les 3 scénarios les plus probables