L'AFFAIRE XITTEL SURVIVRE AUX DDOS

En 2012, durant trois mois, Xittel a été victime de plusieurs attaques virulentes par DDOS qui ont paralysé ses services. Elle a eu recours à l'aide de plusieurs intervenants pour contrer ces menaces. C'est la solution matérielle de Radware qui a permis à l'entreprise d'assurer sa défense.

L'équipe de *SÉCUS* a rencontré Sylvain Gélinas, vice-président des opérations chez Xittel, et relate cette histoire étonnante.

PROPOS RECUEILLIS PAR MARIO AUDET

À PROPOS DE XITTEL

Basé à Trois-Rivières, Xittel, fournisseur d'accès Internet, emploie 80 personnes et compte 15000 clients résidentiels et commerciaux localisés partout au Québec. L'entreprise offre à sa clientèle résidentielle des services Internet, la téléphonie IP et la câblodistribution. À sa clientèle d'affaires, Xittel propose l'hébergement Web, la téléphonie IP, l'Internet haute vitesse et divers services en ligne. Ainsi, ses services aux entreprises diffèrent : centre d'appels pour compagnies d'assurance, service de répartition pour pompiers, etc.

AU COMMENCEMENT

Les attaques de Xittel ont débuté le 25 novembre 2012. À ce moment, les liens de communication de l'entreprise ont complètement été submergés par du trafic illégitime. Il n'était plus possible de transmettre des informations et tout le trafic qui entrait ne servait à rien. La firme ne comprenait pas, car c'était la première fois qu'elle vivait un incident aussi important.

Le lendemain, l'histoire s'est répétée, puis le surlendemain. Pendant plusieurs jours (jusqu'au 14 décembre), Xittel constatait que les attaques visaient un client spécifique. Ne sachant quoi faire, la firme a débranché sporadiquement le client visé. Elle a été contrainte de demander à ce dernier de se trouver un autre fournisseur de services puisqu'elle n'avait pas les moyens de se protéger contre ces attaques.

Le 25 décembre au matin, les attaques ont recommencé de plus belle. Cette fois, un autre client hébergé était ciblé. « Nous croyions avoir réglé le problème, mais nous avons réalisé que nous étions la cible », a déclaré Sylvain Gélinas, responsable de la gestion de cette crise.

FAIRE FACE À LA TEMPÊTE

Durant les trois mois qui ont suivi, Xittel subissait des attaques. L'entreprise a dû développer une recette pour se protéger : blocage du périmètre, redirection et segmentation du trafic, etc.

Xittel a aussi demandé de l'aide à ses cinq fournisseurs de bande passante, mais ces derniers n'ont pas été collaboratifs de la même façon :

- Le premier avait déjà délesté Xittel comme client.
- Le second avait offert son aide, mais invitait Xittel à se trouver un autre fournisseur.
- Le troisième mentionnait que peu importe ce qui se passait (bon ou mauvais trafic), Xittel allait devoir payer.
- Le quatrième a offert son aide, mais allait transmettre une proposition dans deux semaines.
- Le dernier avait offert une collaboration immédiate.

Dans de telles conditions, Sylvain Gélinas anticipait en désespoir de cause que la situation problématique allait durer de six mois à un an !

LES COMMUNICATIONS AVEC LA CLIENTÈLE

Durant cette période, le centre d'appels de Xittel est passé de 1000 à 6000 appels par jour. Il faut comprendre que certains clients n'avaient plus de téléphone durant cette crise pour pouvoir communiquer avec Xittel (puisqu'ils utilisaient le service de téléphonie IP de l'entreprise).

Selon M. Gélinas, outre les abonnés grand public, certains clients d'affaires avaient VRAIMENT besoin d'avoir un accès Internet. Pour Xittel, c'était requis pour la survie de l'entreprise. Ainsi, les membres de l'équipe de direction et des ventes ont dû s'entretenir avec les clients pour les rassurer. « Le travail de l'équipe auprès des clients a été incroyable », mentionne M. Gélinas.

L'EXPÉRIENCE AVEC RADWARE

En plus de la recette utilisée, Xittel devait se tourner vers une solution technologique. Elle a sollicité plusieurs fabricants pour qu'ils lui présentent des produits. Dans le contexte, Xittel était victime. Sylvain Gélinas explique que son employeur ne s'est donc pas lancé dans un vaste processus de sélection. Ainsi, plusieurs boîtes de produits à expérimenter se sont empilées chez Xittel.

La solution retenue ? Celle de Radware. « Radware était la seule entreprise pouvant répondre à tous les besoins de Xittel », déclare M. Gélinas. Radware permettait au fournisseur Internet de faire ce qui suit :

- disposer d'une solution rapidement (Defense Pro) ;
- offrir une solution permettant de bloquer rapidement les attaques par DDOS et transmettre des alertes ;
- avoir recours à une équipe d'intervention d'urgence (*Emergency Response Team*) de Radware basée en Israël pouvant donner du soutien en ligne ;
- rediriger le trafic « sale » chez Radware pour faire le ménage et de retransmettre le trafic propre.

Dans le cas de la redirection du trafic, M. Gélinas précise ceci : « J'étais le premier surpris de cette redirection, mais ça marche ! »

Xittel a beaucoup aimé que Radware dépêche un représentant sur place (Dominique Clément) et fournisse le soutien d'une personne (Jocelyn Rainville) faisant le lien avec l'équipe. « Il y a certains fabricants qui nous ont transmis une boîte par Purolator et ils nous ont mentionné de les appeler lorsque Xittel serait prête à la mettre en service », ajoute M. Gélinas.

L'INTERVENTION DE RADWARE

Lorsque Dominique Clément de Radware s'est présenté chez Xittel, il a vite senti le stress vécu par les gens qu'ils rencontraient. Il connaissait depuis plusieurs semaines la situation de crise de l'entreprise.

Fait cocasse : la boîte a été installée en plein jour. Comme M. Gélinas et M. Clément se plaisent à le raconter, la dorsale de Xittel était en arrêt et le branchement du Defense Pro s'est fait en « cinquante millisecondes ». La pression sur les installations de Xittel a diminué de 50 % après une journée. Au cours des jours suivants, la boîte a appris du trafic qui circulait et a effectué des blocages. Ainsi, son pourcentage d'efficacité a considérablement augmenté.

Les attaques contre Xittel ont pris fin le 21 février 2013 grâce à l'arrestation de l'individu qui les commettait.

Sylvain Gélinas de Xittel et Dominique Clément de Radware

CE QUI A CHANGÉ

Depuis cet incident, selon M. Gélinas, l'organisation travaille différemment. Les diverses équipes ont été éprouvées par les attaques et elles sont maintenant plus soudées. Elles travaillent dorénavant plus ensemble. Elles font plus de veille et de surveillance qu'auparavant quant aux attaques par DDOS. Elles sont plus au courant des nouvelles attaques.

À ce sujet, M. Gélinas affirme que Defense Pro de Xittel bloque en ce moment une attaque à la minute. Il a constaté qu'il y a six mois, leur infrastructure subissait une attaque de plus d'un Go aux six mois. Maintenant, elle subit trois attaques de ce type chaque mois. « Demeurez alerte, car les attaques continueront et changeront de forme. Cette tendance va exploser ! » prévient M. Gélinas. Ce dernier ajoute que les organisations peuvent se défendre et qu'elles ne sont pas des victimes sans défense. « Il y a des gens qui peuvent nous aider dans l'industrie. Il y a des équipements qui peuvent surveiller les attaques et nous protéger. Il y a des services comme ceux de Radware qui peuvent vous aider. Nous ne les avons choisis pas pour rien », conlut M. Gélinas, satisfait. ■

CARACTÉRISTIQUES DES ATTAQUES CONTRE XITTEL

- 200 attaques par DDOS pendant trois mois – 1 à 45 attaques par jour ;
- 22 000 zombienets (*botnets*) utilisés pour attaquer Xittel;
- 5 à 10 Gbps de données simultanément;
- chaque attaque durait de 60 à 120 minutes de façon très bien chronométrée;
- les vecteurs d'attaques étaient variables.

Sylvain Gélinas, de Xittel, et Dominique Clément, de Radware, vous invitent à assister à la présentation qu'ils donneront au CQSI 2013. Ils fourniront alors des détails sur « L'affaire Xittel » et présenteront les différents moyens utilisés pour effectuer des attaques par DDOS.