Atos Wordline et Crédit Mutuel victimes d'un détournement de trafic IP

Mise à jour le 2/05 à 19h10 (commentaires de Worldline sur l'incident)

Dans la nuit de mercredi à jeudi dernier, le trafic Internet de 37 organisations – issues des services financiers ou de la technologie majoritairement – a été détourné vers Rostelecom, un opérateur russe dont 49 % du capital est contrôlé par l'Etat. Parmi les victimes de ce détournement, on trouve notamment Worldline France et Allemagne, Euro-Information, le GIE informatique de Crédit Mutuel – CIC, et Docapost, une filiale de La Poste focalisée sur le traitement de documents. Le spécialiste du traitement des transactions financières d'Atos et la DSI de la banque figurent parmi une liste assez impressionnante d'institutions financières victimes de ce détournement. On y retrouve ainsi Visa, HSBC, UBS, Fortis ou Mastercard. Les sociétés de technologies EMC, Verisign (qui exploite les serveurs racines du DNS) et Symantec font aussi partie des victimes.

Dans le cas de Worldline et du Crédit Mutuel – CIC, le détournement de trafic a duré de 0h36 (heure de Paris) à 6h25. L'anomalie a été un peu plus courte chez Docapost, où les flux normaux ont été restaurés vers 5h20. Worldline conteste toutefois ces données issues de l'outil de suivi d'incidents de BGPmon, le prestataire spécialisé dans la surveillance des flux BGP qui a donné l'alerte. Le spécialiste de la gestion des transactions parle d'une interruption du trafic Internet de moins de 7 minutes dans la nuit du 26 au 27 avril. Un porte-parole d'Atos explique que l'incident a été limité à certaines adresses uniquement et qu'il serait dû à « *un opérateur externe qui a reconnu être à l'origine de l'erreur lors d'une migration planifiée* ».

Détournement intentionnel du trafic ?

Si les circonstances précises entourant cet épisode restent mystérieuses, les causes techniques de ce détournement sont connues. Elles résident dans le protocole BGP (Border Gateway Protocol) qui route d'importants volumes de trafic réseau sur les backbones d'Internet, entre les FAI et autres grands réseaux composant le Net. Avec ce protocole, les fournisseurs de services peuvent déclarer transporter, par erreur la plupart du temps, des pans de trafic sur lesquels ils n'ont aucun droit. Malgré diverses propositions techniques pour corriger cette lacune technique, BGP reste aujourd'hui exposé à des erreurs humaines de configuration… mais aussi à des détournements intentionnels. De telles opérations permettant de récupérer – et éventuellement de copier et/ou modifier – de grands volumes de données. Et, même si le chiffrement limite l'intérêt de telles opérations, l'exploitation des métadonnées fournit des renseignements intéressants sur les entités ciblées.

En 2013, Renesys (entretemps racheté par le spécialiste DNS Dyn) expliquait que les détournements de trafic intentionnels étaient très courants. Les failles de BGP permettant de faire passer un trafic tiers par son réseau pour ensuite l'acheminer à son propriétaire légitime, qui n'en aura alors pas conscience.

Dans le cas du détournement du 26 avril dernier (dont on peut voir une modélisation graphique

ici), BGPmon note que la liste des victimes pose question, du fait de la surreprésentation des institutions financières. Tout comme le fait que l'opérateur vers lequel tout ce trafic a soudain été dirigé a déclaré de nouvelles routes, laissant à penser qu'il ne s'agit pas d'une mauvaise manipulation. Même si, dans son billet de blog, BGPmon ne se prononce pas définitivement, relevant qu'il pourrait s'agir tant d'un détournement intentionnel que d'une erreur de configuration réseau. Pour l'heure, le prestataire a classé l'incident comme un « *possible détournement* ».

A lire aussi :

Vault 7 : Wikileaks lève le voile sur les méthodes d'écoute de la CIA

Trois failles zero day d'iOS servaient à espionner des dissidents

crédit photo © Alexei Tacu – Shutterstock