ProtonMail cède au chantage pour faire cesser une attaque DDoS | Le Net Expert Informatique

	ProtonMail cède au chantage pour faire cesser une attaque DDoS

Le service de Webmail sécurisé a révélé avoir été victime d'une attaque DDos d'ampleur au cours de la semaine. Pour faire cesser l'attaque, la société a accepté de payer la rançon exigée par les attaquants, mais l'attaque a continué malgré le versement de l'argent.

Payer la rançon, cela ne marche pas forcément. Le service de mails chiffrés ProtonMail en a fait l'expérience cette semaine : victime d'une attaque DDoS d'ampleur les visant en premier lieu, mais touchant également des services tiers hébergés sur la même infrastructure, le service mail a expliqué dans une note de blog avoir accepté de payer la rançon exigée par le groupe de hackers, sous la pression d'autres sociétés. Malheureusement, le versement des 6000 dollars en bitcoin n'a pas suffi à mettre fin à l'attaque et l'hébergeur a été contraint de mettre le service mail hors ligne pour limiter l'impact. Le service ProtonMail compte environ 500.000 utilisateurs : celui-ci est basé en Suisse et entend apporter aux utilisateurs une solution supposée sécurisée et capable de mettre des bâtons dans les roues de la NSA et d'autres agences de renseignement.

La pression des pairs

Dans un post de blog, ProtonMail explique avoir fait l'objet depuis le 3 novembre d'une importante attaque DDoS en plusieurs phases, qui l'a finalement conduit à mettre ses services hors ligne temporairement.

Sur son blog, ProtonMail décrit une attaque en deux temps : une première attaque a brièvement mis le site hors ligne dans la nuit du 3 novembre. Cette attaque avait été précédée par un premier mail exigeant une rançon. L'attaque a repris le lendemain vers 11h du matin et l'hébergeur du service mail a alors commencé à prendre des mesures afin de canaliser le trafic malveillant qui visait les services de ProtonMail.

L'attaque s'est par la suite complexifiée comme le remarque le service : vers 2 heures de l'après-midi, les attaquants ont commencé à viser les points « sensibles » de leur datacenter et de leur fournisseur d'accès tels que les routeurs placés à Zurich ou Francfort. Une attaque qui excédait selon la société 100 Gbps de débit et qui a fini par faire plier le datacenter et forcer le fournisseur d'accès à mettre hors ligne une partie de leur équipement. La manœuvre a donc affecté de nombreuses entreprises ayant recours à la même infrastructure que ProtonMail.

Et la situation s'est alors compliquée pour ProtonMail, qui explique sur son blog avoir dû faire face à de nombreuses pressions de la part d'autres entreprises touchées par l'attaque. « À contrecœur, nous avons accepté de payer dans l'après-midi. Nous espérions qu'en payant la rançon, nous pourrions ainsi épargner les entreprises touchées par l'attaque qui nous visait, mais l'attaque a pourtant continué » explique la société sur son blog.

Plus compliqué que prévu

Prenant contact avec les autorités suisses, la société explique avoir découvert que l'attaque se révélait plus complexe que prévu : d'une part, la première phase de l'attaque correspondait au modus operandi d'un groupe de cybercriminels identifié par les autorités suisses, le collectif Armada. Celui-ci avait déjà été signalé par le Cert suisse et semble avoir pratiqué plusieurs attaques DDoS contre d'autres entreprises nationales, en exigeant une rançon pour faire cesser l'attaque. La seconde phase de l'attaque est en revanche bien plus complexe et ne semble pas être liée au collectif Armada, laissant ProtonMail envisager la possibilité d'une attaque menée par un gouvernement à leur encontre.

ProtonMail rappelle que l'attaque DDoS a simplement causé l'arrêt du service, mais que les données des utilisateurs restent sécurisées. La société est actuellement en recherche de solutions afin de faire face à un DDoS de cette ampleur et expliquait hier sur son compte Twitter être en train de rechercher un datacenter « suffisamment courageux » pour les héberger. En parallèle, la société a lancé une campagne de crowdfunding afin de mettre en place des mesures lui permettant de maintenir son service à flot malgré l'attaque. Les attaques se poursuivaient ce matin. Le service reste ponctuellement perturbé par l'attaque, mais le site est encore accessible par intermittence.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/protonmail-cede-au-chantage-pour-faire-cesser-une-attaque-ddos-39827816.htm