Votre box pourrait bien être utilisée pour des piratages d’envergure…

	Votre box pourrait bien être utilisée pour des piratages d’envergure…

Le groupe LizardSquad, qui a notamment orchestré les attaques Ddos sur le PSN et Xbox Live à Noël, a dévoilé peu de temps après une offre payante offrant des attaques par déni de service à la demande. Un « service » qui repose essentiellement sur des routeurs privés mal sécurisés.

Le 25 décembre, le groupe LizardSquad lançait une attaque Ddos contre les services en ligne du Playstation Network et du Xbox Live. Dieu merci (ou pas) Kim Dotcom est venu à la rescousse des utilisateurs et tout est rapidement rentré dans l'ordre. Mais peu de temps après, LizardSquad lançait une offre de Ddos payante à la demande, expliquant que ses récentes attaques largement relayées dans la presse n'étaient en fait qu'une opération de communication visant à faire preuve de l'efficacité de leurs techniques.

Business is business, as usual

L'offre présentée par LizardSquad vous permet, contre espèces sonnantes et trébuchantes (mais ils acceptent aussi les bitcoins) de lancer une attaque Ddos sur la cible de votre choix. Le tout sans avoir à s'embarrasser des aspects techniques : le groupe de pirates se charge de tout, vous offrant ainsi un service clef en main pour mettre des bâtons dans les roues de vos concurrents, ennemis, amis, bref, à peu près tout ce qui est en mesure de proposer un service en ligne et qui vous dérange. Officiellement, l'outil LizardStresser est avant tout pensé pour les utilisateurs souhaitant tester la robustesse de leurs services face à une attaque Ddos.

Un exemple des prix pratiqués par LizardSquad (Crédit original de l'image : The Register)

Le journaliste Brian Krebs, spécialisé dans la cybersecurité, s'est lancé dans une petite croisade contre ce groupe de pirate. Il avait dans un précédent article entrepris de révéler l'identité de certains d'entre eux et n'hésitent pas à les qualifier de « script kiddies », un terme péjoratif qui désigne les débutants sans connaissances réelles qui récupèrent et utilisent des programmes clef en main pour s'attaquer à des sites web ou des internautes. De part et d'autre, les insultes volent, LizardSquad n'hésitant pas à affirmer que leurs serveurs sont hébergés « quelque part sur le front de Brian Krebs »

Brian Krebs s'est penché sur les méthodes utilisées par le groupe pour mener à bien leurs attaques Ddos. En effet, plusieurs options sont disponibles pour parvenir un tel résultat : certain ont recours à des botnets, Anonymous de son coté s'était fait remarquer pour l'utilisation du soft LOIC qui transformait ses utilisateurs en « botnet consentant » et d'autres méthodes reposant sur l'exploitation de failles de sécurité sont également utilisées (On pense notamment à la technique de l'amplification DNS)

Routeurs domestique : l'ennemi intérieur ?

LizardSquad dispose lui aussi de son propre réseau Botnet pour mener à bien ses attaques, explique Brian Krebs, mais celui-ci est essentiellement constitué de routeurs domestiques. L'auteur explique être parvenu, avec l'aide de chercheurs non cités, à mettre la main sur le malware utilisé par LizardSquad. Celui-ci est une version modifiée d'un trojan signalé auparavant par la firme russe Dr.Web.

Krebs remarque que ce malware a pour fonctionnalité de scanner l'ensemble du réseau afin de trouver les routeurs ayant gardé leurs paramètres d'usine. En effet, la plupart des utilisateurs négligent la sécurité de leurs routeurs wifi, et si les mots de passe configurés en usine n'ont pas été changés, accéder à l'interface n'a rien de compliqué.

Le malware n'est pas spécifique aux routeurs domestiques, explique Krebs, il est conçu avant tout pour s'attaquer aux machines utilisant Linux. Le journaliste explique que les routeurs domestiques constituent la majeure partie du botnet de LizardSquad, mais que les routeurs de certaines universités et entreprises sont probablement infectés.

Si vous craignez que votre paisible routeur domestique ne soit en réalité un agent double à la solde de LizardSquad, Krebs détaille également dans la suite de son article les techniques de base permettant de sécuriser l'accès à son routeur. La plus simple et la plus efficace reste néanmoins la plus évidente : changer ses mots de passe.

L'article de Brian Krebs :
http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/#more-29431

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/lizardsquad-devoile-un-service-de-ddos-a-la-demande-qui-s-appuie-sur-les-routeurs-39812835.htm
Par Louis Adam