Les smart TV vulnérables à l'attaque « bouton rouge »

Les spécialistes de la sécurité sont unanimes : non les menaces n'ont pas changé, mais elles disposent d'une surface de jeu beaucoup plus grande. Après les systèmes industriels (les fameux SCADA) ou les smartphones, c'est au tour des **smart TV** d'intéresser les cybercriminels. Une attaque a été découverte par **Yossef Oren** et **Angelos D. Keromytis**, deux chercheurs de l'université de Columbia au département Network Security Lab. Ils feront leur démonstration à l'occasion de la conférence sur la sécurité Usenix, prévue au mois d'août à Washington. Ils en ont cependant mis un extrait sur le web.

Cette attaque dénommée « **Bouton rouge** » par les universitaires (en référence à la couleur du bouton qui commande les fonctionnalités interactives de l'écran) utilise **deux failles dans le standard HbbTV** (hybrid broadcast-broadband) qui est présente sur la majorité des téléviseurs connectés en Europe. Les diffuseurs et les annonceurs poussent ce standard, car il permet un meilleur ciblage publicitaire et d'ajouter du contenu interactif comme des sondages, des applications ou des jeux. Ce standard est promu par le consortium **DVB** (Digital Video Broadcasting). Les chercheurs soulignent que *« les spécifications et leurs implémentations en temps réel font que le système est non sécurisé »*.

Investissement faible pour dégâts considérables

Une des failles porte sur le fait que le logiciel ou le contenu incorporé (en mode HTML) dans le flux de diffusion HbbTV **n'est pas lié à un serveur web** et n'a donc pas d'origine identifiée. Selon eux, « *il suffit d'une **injection géolocalisée via des fréquences radios** pour réaliser une attaque de grande ampleur. Elle nécessite une infrastructure à faible coût et elle est très difficile à détecter* ». Sans dévoiler la méthode, ils estiment qu'avec un **budget de 450 dollars**, ils peuvent toucher **20 000 smart TV** dans une zone urbaine dense (environ 1,4 km²). Cette échelle peut être augmentée en prenant du matériel plus élaboré et relayer par un drone. Ils soulignent une différence avec les attaques traditionnelles sur l'Internet des objets. « *Ce procédé utilise le réseau physique pour attaquer le réseau des données, alors que dans l'Internet des objets, c'est souvent le contraire* ».

Selon un entretien réalisé par nos confrères de *Forbes*, les chercheurs ont trouvé cette faille dans une attaque contre le standard en décembre dernier. Interpellé sur ce bug, l'organisme de standardisation a estimé que ce problème n'était pas suffisamment grave pour modifier HbbTV. Pour autant, les deux universitaires estiment que le risque n'est pas moindre et que l'investissement pour réaliser l'opération est très abordable. L'attaque qui s'apparente à une offensive de type **man in the middle** peut avoir de multiples objectifs : vols d'identifiant sur certains sites (Facebook, Twitter), coupure de l'accès à Internet, diffusion de fausses informations, etc. Pour tenter d'échapper à cette menace, les deux scientifiques prônent la mise en place d'une vraie **surveillance du réseau** des smart TV, mais aussi l'intégration d'un **système de validation des applications** qui sont téléchargées sur les postes.

A lire aussi :

Un consortium américain autour de l’Internet des Objets

Android à la conquête des Smart TV avec le nouveau SoC de Marvell