

# Comment pirater la reconnaissance faciale

## ?

Attaque de face contre la reconnaissance du visage. Le **docteur Nguyen Minh Duc**, expert vietnamien a démontré qu'il était possible de passer outre les moyens de [visualisation faciale](#) avec de simples photographies imprimées.

C'est lors de la conférence de sécurité **Black Hat de Crystal City** (Virginie) que l'équipe de chercheurs du centre vietnamien **Bach Khoa Internetwork Security** (Bkis) a dévoilé cette **vulnérabilité**. Cette technologie biométrique utilisée notamment sur des portables des marques [Lenovo](#), **Asus** et **Toshiba** a donc été passée à la moulinette par les experts.

En détail, la reconnaissance est un simple logiciel qui numérise un visage, en extrait les points remarquables et les **compare aux empreintes numériques déjà enregistrées**. Utilisée pour éviter le recours aux traditionnels logins et mots de passe, la [technologie](#) montre là ses limites.

Pour preuve, ils ont publié une vidéo de leur exploit librement visible sur le site du **Black Hat**.

A l'appui de leur trouvaille, les chercheurs ont établi des « **degrés d'inefficacité** » des logiciels de reconnaissance. La palme du plus mauvais revient alors au **Veriface III de Lenovo** (une photo en noir et blanc étant seulement nécessaire). Concernant l'**Asus SmartLogon V1.0.0005**, les chercheurs ont expliqué devoir : « *modifier la luminosité ainsi que l'angle de la prise de vue* » .

Enfin le logiciel le plus compliqué à détourner a été le « **Toshiba Face Recognition 2.0.2.32** » à en croire les chercheurs. Sur le site de la conférence, ils expliquent qu'ils ont dû « *tester une série d'impressions avec des **effets de lumière et des angles de vue différents** avant de pouvoir pénétrer le système* » .

Cette démonstration n'est pas nouvelle puisque déjà en 2004, le **CCC (Chaos Computer Club)** avait déjà réussi à pirater un système similaire avec quelques outils simples. Un piratage simple comme un sourire.