Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n°18 Octobre 2015

Ce « flash » de l'ingérence économique évoque des actions dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :
securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°18 Octobre 2015

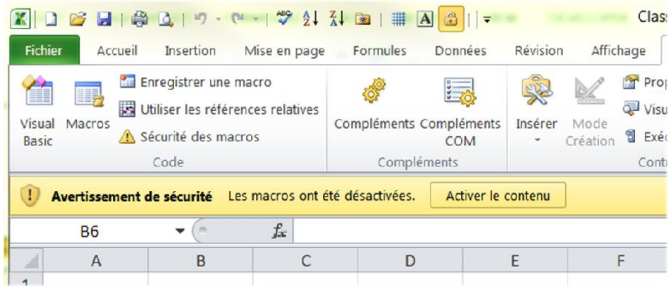
Recrudescence des campagnes de courriels piégés à l'aide de malwares « macros »

Au cours de l'été 2015, la DGSI a constaté la recrudescence de courriels piégés ciblant les entreprises françaises de toutes tailles. Ces campagnes de spams ont utilisé un mode opératoire déjà éprouvé, qui exploite les fonctionnalités de « macros » proposées dans de nombreuses suites bureautiques, notamment Microsoft Office.

Le vecteur de compromission consiste en un courriel accompagné d'une pièce jointe au format « .doc ou .docx » voire « .xls ou .xlsx ». Rédigé dans un français conforme à la règle syntaxique, le courriel piégé évoque généralement des problèmes de factures impayées ou des avis de virement, afin d'inciter le destinataire à ouvrir le fichier joint.

Si la fonctionnalité « macro » est activée par défaut, le téléchargement du malware s'effectuera automatiquement. A l'inverse, si elle est désactivée, la victime, incitée à le faire, déclenchera alors un script qui tentera de se connecter à un serveur à partir duquel il téléchargera et installera le logiciel malveillant directement sur le poste de la victime.

Dans les deux cas de figure, l'infection se réalisera de manière transparente pour l'utilisateur.



Le logiciel malveillant le plus connu de ce type se nomme **Dridex**, un cheval de Troie bancaire. Il en existe de nombreuses variantes. Sa finalité consiste à subtiliser les données bancaires présentes - ou saisies - sur le poste informatique qu'il infecte, pour permettre ensuite aux cybercriminels d'effectuer des virements bancaires frauduleux. Il peut également cibler d'autres types d'informations personnelles (*par exemple, identifiants et mots de passe de connexion à différents sites Internet*).

Ce même vecteur de compromission peut également être utilisé pour propager d'autres types de malwares : rançongiciels (*cf. Flash Ingérence n°9 – 10 mars 2014*), logiciels d'espionnage – en vue d'exfiltrer toute information – ou de prise de contrôle à distance par des cybercriminels.

Commentaire :

Apparu voici une dizaine d'années, ce mode opératoire repose essentiellement sur des capacités d'ingénierie sociale et s'avère d'une efficacité redoutable. En effet, ces courriels, accompagnés d'une pièce jointe piégée, n'exploitent aucune vulnérabilité mais bien une fonctionnalité légitime – la « macro » –, ce qui explique pourquoi les solutions d'antivirus ne les détectent pas comme des logiciels malveillants.

Les préjudices subis par les entreprises à la suite de telles intrusions ne sauraient être minimisés : vol de données bancaires ouvrant la voie à des escroqueries aux ordres de virement, perte de données stratégiques, coût et temps de remise en état des postes infectés, perte de confiance des clients et partenaires, voire mise en péril de la société.

Préconisations de la DGSI :

Afin de se prémunir contre de telles actions, la DGSI recommande d'appliquer les règles d'hygiène informatique suivantes :

- Désactiver l'exécution automatique des « macros » dans les logiciels bureautiques. Depuis Office 2010, il s'agit de la configuration par défaut ;
- Rester vigilant avec la messagerie électronique. En cas de doute, ne pas ouvrir les pièces jointes accompagnant les courriels non sollicités ou provenant d'un expéditeur incertain, voire inconnu ;
- Mettre à jour régulièrement le système d'exploitation et les anti-virus (ainsi que les bases de signatures) des postes de travail et des serveurs informatiques ;
- Effectuer des sauvegardes régulières ;
- Sensibiliser les utilisateurs à ce type de spams.

En cas de suspicion d'infection, il est conseillé de :

- Vérifier la légitimité des dernières et futures transactions bancaires ;
- Signaler immédiatement à sa banque le risque potentiel de fraude aux ordres de virement ;
- Changer en priorité les mots de passe d'accès aux comptes bancaires en utilisant un autre poste que celui qui a été infecté.