Sécurité économique territoriale

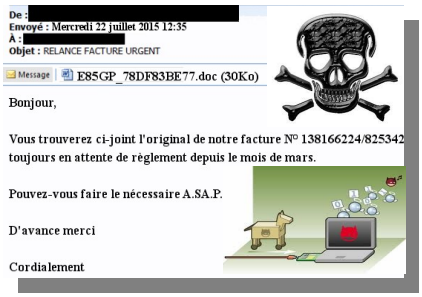
Rhône-Alpes

MESSAGE D'ATTENTION

« TROJAN *DRIDEX ou DRIXED* »

Courant juillet 2015, une entreprise rhônalpine est victime d'une quinzaine de prélèvements frauduleux réalisée à l'aide de faux ordres de virement à destination de comptes basés à l'étranger. Le préjudice avoisine les 520 000 €.

Après enquête interne, une intrusion informatique a été détectée. Le service comptabilité a reçu un courriel se présentant comme étant une relance de facture avec en pièce jointe ladite facture. Une fois ouvert, ce document a véhiculé un logiciel malveillant ayant permis aux malfaiteurs de récupérer toutes les informations nécessaires pour passer à l'acte.


De : [redacted]
Envoyé : Mercredi 22 juillet 2015 12:35
À : [redacted]
Objet : RELANCE FACTURE URGENT

Message | E85GP_78DF83BE77.doc (30Ko)

Bonjour,

Vous trouverez ci-joint l'original de notre facture N° 138166224/825342 toujours en attente de règlement depuis le mois de mars.

Pouvez-vous faire le nécessaire A.SA.P.

D'avance merci

Cordialement

DE QUOI PARLE-T-ON ?

Une importante vague d'attaques par pourriels touche actuellement les sociétés françaises. Les e-mails, à entête de banques, d'administrations ou d'entreprises, sont rédigés dans un français correct. Ils appellent à régler rapidement une facture impayée. La notion d'urgence évoquée dans l'objet et le texte incite le destinataire à ouvrir la pièce jointe.

Ce document, enregistré au format « *.doc, .docx, .xls, .xlsx ou PDF* », est souvent nommé d'une suite de chiffres, de caractères spéciaux et de lettres aléatoires (*exemple : E85GP_78DF83BE77.doc*). A l'ouverture, soit la page est totalement blanche, soit elle est constituée de caractères indéchiffrables.

Dans le même laps de temps, un code d'attaque déclenche automatiquement l'installation d'une application malveillante (*logiciel espion, un trojan bancaire ou un cryptoware*), via un *script Visual Basic,* laquelle ne sera pas détectée par les antivirus. Les opérations bancaires alors réalisées se font à l'insu de l'utilisateur.

DRIDEX (ou DRIXED) n'affecte que les ordinateurs fonctionnant sous système d'exploitation Microsoft Windows. Une fois infecté, le trojan dérobe les données bancaires et informations personnelles mais permet également la prise de contrôle à distance de la machine.

QUE FAIRE ?

En amont : Maintenir à jour le système d'exploitation et l'antivirus.
- **Installer une solution antimalware pour réduire les risques.**
- **Désactiver l'exécution automatique des macros des suites bureautiques.**

Lors de la réception de courriels : Se montrer vigilant dans le traitement de la messagerie.
- **Ne pas ouvrir de pièce jointe provenant d'une personne non identifiée.**
- **Faire preuve de méfiance dès lors qu'une pièce jointe porte un nom inhabituel.**
- **Ne jamais transférer un mail suspect pour qu'un collègue tente de l'ouvrir, cela étendrait la contamination.**

En cas d'infection : Le trojan *DRIXED* ou *DRIDEX* se lance n'importe quand et peut rester inactif durant un certain temps. Donc, si vous avez reçu un mail suspect et ouvert la pièce jointe, pour tenter de neutraliser ce malware avant qu'il n'entre en action, il convient de :
- **Prévenir immédiatement le responsable informatique de l'entreprise.**
- **Effectuer rapidement une mise à jour de l'anti-virus.**
- **Déconnecter l'ordinateur du réseau en débranchant le câble ou en arrêtant la connexion Wifi mais surtout ne pas éteindre la machine.**
- **Lancer une analyse anti-virus du poste puis procéder à un nettoyage à l'aide d'outils gratuits tels que « *Mbar* » ou « *ADWcleaner* ».**
- **Consulter le site : https://lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/**
- **Changer immédiatement le mot de passe d'accès au compte bancaire ainsi que tous les logins et mots de passe d'accès à des services en ligne depuis un autre moyen de connexion que l'ordinateur suspecté d'infection.**
- **Alerter rapidement votre banque pour tenter de faire bloquer les éventuels virements.**

En cas de problème avéré ou de simple tentative :

***Déposer rapidement plainte* auprès du service de police ou de gendarmerie territorialement compétent.**

Lettre électronique **N° 8** éditée par la région de gendarmerie de Rhône-Alpes – 36 bd de l'Ouest – 69580 Sathonay-Camp - ☎·: 04.37.85.21.15
Rédaction : Cellule Intelligence Économique régionale