Emotet reprend du service : ce trojan bancaire devenu malware à tout faire

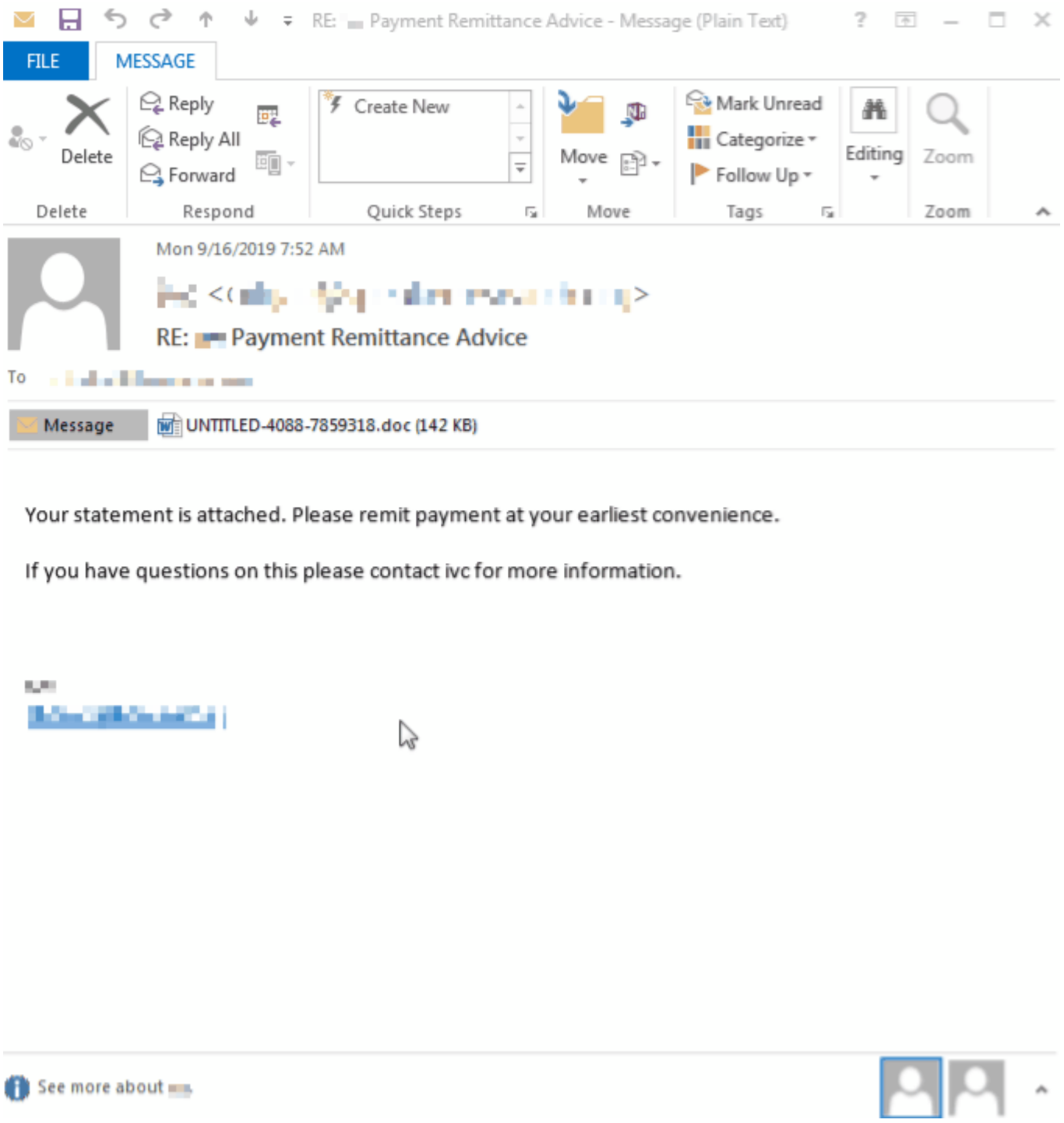
Plusieurs éditeurs de solutions de sécurité l'ont signalé ces derniers jours : Emotet est de retour.

Identifié pour la première fois en 2014, ce cheval de Troie bancaire* est devenu depuis lors une plate-forme de diffusion de spam et de *malware*. Il est notamment l'un des vecteurs de propagation du rançongiciel Ryuk.

Les premières versions reposaient sur un script mis en pièce jointe d'e-mails imitant des avis de paiement, des rappels de factures ou encore des notifications de suivi de colis.

Les sources d'infection se sont progressivement diversifiées. Notamment à travers l'utilisation des macros dans les logiciels de la suite Microsoft Office.

Le cas se présente actuellement. Après un « break estival », Emotet a recommencé à sévir, en s'appuyant sur des documents Word. Pour en consulter le contenu, les utilisateurs sont invités à… activer les macros.



Pour ne pas éveiller les soupçons de ses cibles, Emotet s'immisce dans des conversations qu'elles ont eues par le passé. De plus en plus souvent, il met le nom de la victime en objet.

Emotet : un air de WannaCry

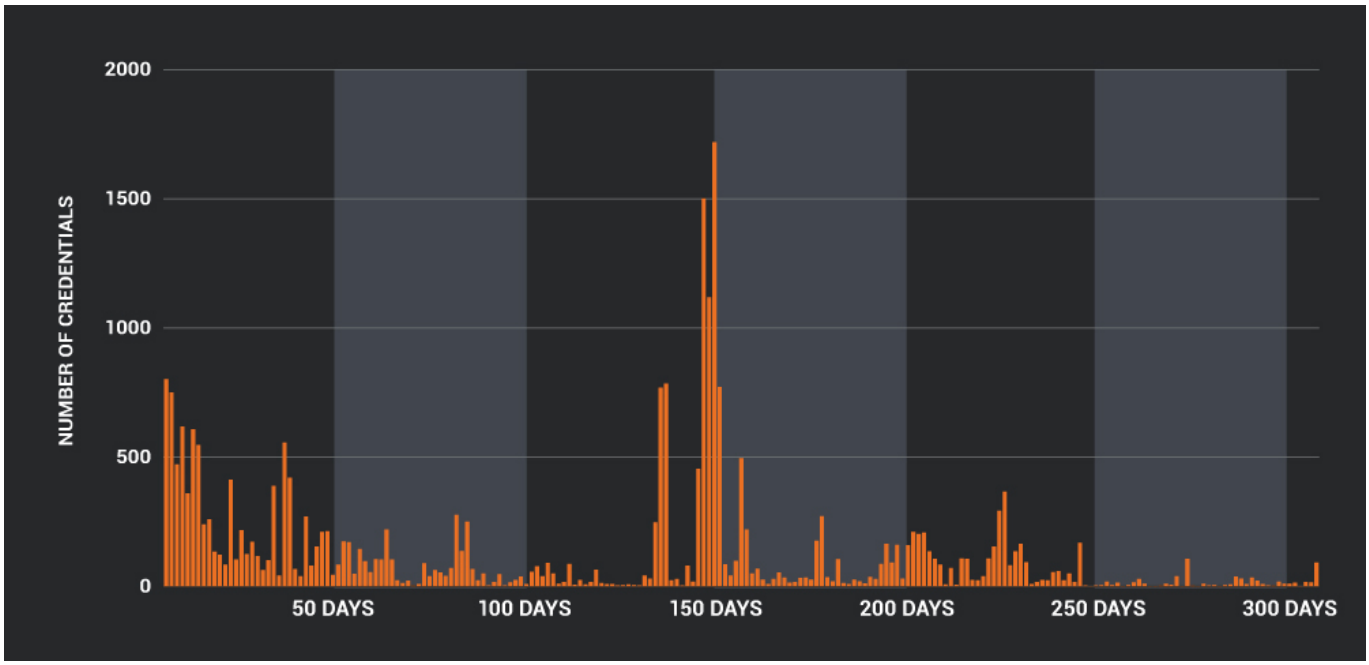
Capable de détecter les VM et les bacs à sable, Emotet est aussi polymorphe. En d'autres termes, il peut changer sa représentation pour échapper aux détections basées sur les signatures.
Le registre Windows et le planificateur de tâches lui permettent d'établir une persistance sur les systèmes infectés.

Pour se propager sur des réseaux, il recourt à plusieurs outils signés NirSoft :

- NetPass, destiné à récupérer tous les mots de passe réseau pour la session Windows en cours
- WebBrowserPassView, pour faire de même dans les principaux navigateurs web
- Mail PassView, pour les clients de messagerie

Les données d'identification collectées par ce biais sont communiquées à un « énumérateur » qui les teste sur les ressources réseau. Et qui cherche, en parallèle, d'éventuels volumes accessibles en écriture sur SMB *via* les exploits DoublePulsar et EternalBlue (qu'utilisent aussi WannaCry et NotPetya).

La durée de vie de ces identifiants est d'environ une semaine, d'après Cisco Talos. Emotet les transmet à certaines machines infectées pour qu'elles envoient à leur tour du spam.



** Ses premières cibles furent des banques allemandes et autrichiennes. Puis vinrent des homologues suisses. Les attaques se sont mondialisées depuis lors.*