Alerte ! Campagne de pourriels avec documents Microsoft Office malveillants | Le Net Expert Informatique

	Alerte ! Campagne de pourriels avec documents Microsoft Office malveillants

Le CERT-FR alerte sur des pourriels qui se diffusent depuis une semaine en dépit des filtres antispam : attention aux macros malveillantes qu'ils diffusent !

Depuis une semaine, il est observé à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles antispam est relativement faible.
Ces pourriels embarquent des documents Microsoft Office contenant des macros VBA malveillantes. Ces macros ont pour but d'infecter la victime avec Dridex, qui est un logiciel malveillant de type bancaire.
Selon les échantillons, le téléchargement de Dridex peut être effectué de deux façons différentes :
• la macro VBA télécharge puis exécute un script à partir du site pastebin.com. Ce dernier télécharge ensuite le binaire Dridex à partir d'un serveur malveillant ;
la macro VBA télécharge directement le binaire Dridex à partir d'un serveur malveillant.

Il est intéressant de noter que ces pourriels sont très souvent rédigés dans un français sans faute. Le sujet et le contenu du pourriel mentionnent des problèmes de facturation, dans la plupart des cas, pour inciter la victime à ouvrir la pièce jointe.

Le format utilisé dans cette campagne pour les documents malveillants est peu rencontré. En effet, si l'on connaît déjà bien les formats OLE et OpenXML, deux autres formats moins connus commencent à être de plus en plus utilisés pour la propagation de contenu malveillant. Il s'agit du format XML, déjà mentionné dans le bulletin d'actualité CERTFR-2015-ACT-017, et du format MIME HTML qui est le format utilisé dans cette campagne. Ces deux derniers formats ont l'avantage pour les attaquants d'être souvent moins bien détectés par les antivirus.
Bien sûr, les techniques classiques d'obfuscation du code VBA, telles que celles décrites dans le bulletin d'actualité précédemment mentionné, sont toujours utilisées.
A travers les échantillons qui ont pu nous être remontés, le CERT-FR a pu observer les URLs de téléchargement via pastebin suivantes (toutes les URLs suivantes ont été démilitarisées par l'adjonction du suffixe _BAD_ aux noms de domaines et adresses IP) :
http://pastebin.com._BAD_/download.php?i=2YzPRtum
http://pastebin.com._BAD_/download.php?i=mLeUenhF
http://pastebin.com._BAD_/download.php?i=umC3ngcn
Pour les documents dont la macro VBA télécharge directement Dridex, le CERT-FR a pu observer les URLs de téléchargement suivantes :
http://www.adriatic-stone.hr._BAD_/64/I1.exe
http://g000042A.feroze.com._BAD_/25/I8.exe
Enfin, les échantillons Dridex ainsi récupérés tentent de communiquer avec les serveurs suivants :
https://94.23.53.23._BAD_:2443/
https://176.99.6.10._BAD_:8443/
https://173.230.130.172._BAD_:2443/
https://203.151.94.120._BAD_:4443/
https://31.186.99.250._BAD_:8443/
https://146.185.99.250._BAD_:8443/
https://185.12.95.40._BAD_:7443/
https://50.63.174.16._BAD_:6443/
https://79.143.191.147._BAD_:6443/
https://37.143.9.63._BAD_:4433/
Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
ne pas ouvrir les documents ou les pièces jointes non sollicitées ;
désactiver l'exécution automatique des macros dans les suites bureautiques ;
maintenir le système d'exploitation et l'anti-virus à jour.
La désactivation de l'exécution automatique des macros se paramètre dans le menu suivant :
Fichier / Options / Centre de gestion de la confidentialité / Paramètre du Centre de gestion de la confidentialité / Paramètres des macros / Désactiver toutes les macros avec notifications
Documentation
Recrudescence des attaques par macro « Visual Basic for Applications » dans les documents Microsoft Office – Bulletin d'actualité CERTFR-2015-ACT-017 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-017/index.html
CVE-2012-0158 exploit evades AV in Mime HTML format :
http://blog.malwaretracker.com/2013/08/cve-2012-0158-exploit-evades-av-in-mime.html5
3

Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
• ne pas ouvrir les documents ou les pièces jointes non sollicitées ;
• désactiver l'exécution automatique des macros dans les suites bureautiques ;
• maintenir le système d'exploitation et l'antivirus à jour.

Le bulletin d'actualité du CERT-FR détaille les formats de documents et techniques utilisées ainsi que les parades à mettre en place.
Note :
*VBA : Visual Basic for Application est une implémentation de Microsoft Visual Basic intégrée dans l'ensemble des applications de Microsoft Office.

Pour aller plus loin :
Consulter les bulletins d'actualité sur le site du CERT-FR, le bulletin du 15 juin à : http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-024/index.html

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.ssi.gouv.fr/actualite/campagne-de-pourriels-avec-documents-microsoft-office-malveillants/
Par l'ANSSI