Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 15 juin 2015
N° CERTFR-2015-ACT-024

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-024

1 - Présentations de l'ANSSI au SSTIC

Le symposium sur la sécurité des technologies de l'information et des communications (SSTIC) est une conférence française traitant de sécurité informatique qui s'est déroulée, comme chaque année, à Rennes du 3 au 5 juin 2015.

Au cours de cette conférence réunissant de nombreux experts en sécurité des systèmes d'information, des agents de l'ANSSI ont présenté les résultats de leurs travaux sur différents sujets :

- contrôle de l'intégrité du flot d'exécution d'un programme dès la compilation via instrumentation du langage intermédiaire de LLVM (PICON : Control Flow Integrity on LLVM IR) ;
- état de l'art des mécanismes de protection logiciels et matériels appliqués aux consoles de jeux (Stratégies de défense et d'attaque : le cas des consoles de jeux) ;
- développement d'un système d'exploitation multi-niveaux incorporant de nombreux mécanismes de sécurité et de défense en profondeur (CLIP : une approche pragmatique pour la conception d'un OS sécurisé) ;
- injection de commandes vocales sur ordiphone via l'utilisation de la bande FM et d'un kit main libre (Injection de commandes vocales sur ordiphone) ;
- état des lieux de la sécurité actuelle de TLS et des attaques récentes (SSL/TLS, 3 ans plus tard) ;
- détail des spécificités du standard OpenFlow (implémentation de SDN) et présentation de quelques vulnérabilités (Les risques d'OpenFlow et du SDN) ;
- cloisonnement des applications pour limitation d'accès aux données utilisateur (StemJail : Cloisonnement dynamique d'activités pour la protection des données utilisateur).

Les planches de présentation, les actes complets ainsi que les vidéos sont disponibles dès à présent sur le site de la conférence.

Documentation

- https://www.sstic.org/2015/presentation/control_flow_integrity_on_llvm_ir/
- https://www.sstic.org/2015/presentation/stratgies_de_dfense_et_dattaque__le_cas_des_consoles_de_jeux/
- https://www.sstic.org/2015/presentation/clip/
- https://www.sstic.org/2015/presentation/injection_commandes_vocales_ordiphone/
- https://www.sstic.org/2015/presentation/ssltls_soa_reloaded/
- https://www.sstic.org/2015/presentation/risques_openflow_et_sdn/
- https://www.sstic.org/2015/presentation/stemjail_cloisonnement_dynamique_d_activites_pour_la_protection_des_donnees_u

2 - Campagne de pourriels avec documents Microsoft Office malveillants

Depuis le 8 juin 2015, 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 (très souvent 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 du script VBS 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=1YzPHtum`
- `http://pastebin.com._BAD_/download.php?i=eLm1enkF`
- `http://pastebin.com._BAD_/download.php?i=vmCDsgcn`
- `http://pastebin.com._BAD_/download.php?i=2sFBJeqD`
- `http://pastebin.com._BAD_/download.php?i=QsfRd36A`
- `http://pastebin.com._BAD_/download.php?i=WhcTRLi0`
- `http://pastebin.com._BAD_/download.php?i=bPCnR5rx`
- `http://pastebin.com._BAD_/download.php?i=63F8xJCw`
- `http://pastebin.com._BAD_/download.php?i=79qzRcFp`
- `http://pastebin.com._BAD_/download.php?i=AZ7DtEcG`
- `http://pastebin.com._BAD_/download.php?i=Sw5JsjcA`
- `http://pastebin.com._BAD_/download.php?i=yqMMpJSb`
- `http://pastebin.com._BAD_/raw.php?i=AZ7DtEcG`
- `http://178.33.200.166._BAD_/bt/bt/get2007.php`
- `http://217.12.203.152._BAD_/mkk/ata.txt`

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_/64/11.exe`
- `http://g6000424.ferozo.com._BAD_/25/10.exe`
- `http://olyphia.nl._BAD_/45/47.exe`
- `http://travellersvolunteers.org._BAD_/20/12.exe`
- `http://travellersworldwide.co.za._BAD_/20/12.exe`
- `http://slavenjeffcote.co.uk._BAD_/81/50.exe`
- `http://cauldronprojects.eu._BAD_/81/50.exe`
- `http://milieuboot.be._BAD_/81/50.exe`
- `http://spgroups.com._BAD_/20/12.exe`
- `http://weingut-egert.de._BAD_/99/01.exe`
- `http://atfxsystems.co.uk._BAD_/99/01.exe`
- `http://www.dressurstall-sonnenhof.de._BAD_/99/01.exe`
- `http://prignon.com._BAD_/99/01.exe`
- `http://gervifrais.com._BAD_/554/33.exe`
- `http://storesidf.com._BAD_/554/33.exe`

- http://labriardeentreprises.com._BAD_/554/33.exe
- http://orpibriecomterobert.com._BAD_/554/33.exe
- http://esprit-ktm.com._BAD_/js/write.exe
- http://reggae-est.fr._BAD_/xml/write.exe
- http://excosup.fr._BAD_/error/write.exe
- http://scootpassion.com._BAD_/js/write.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/
- https://195.169.147.79._BAD_:1443/
- https://69.164.213.85._BAD_:1443/
- https://118.174.151.27._BAD_:943/
- https://178.62.25.84._BAD_:449/
- https://162.243.12.14._BAD_:449/
- https://176.9.118.201._BAD_:449/
- https://188.93.73.90._BAD_:449/
- https://91.121.91.221._BAD_:1443/
- https://95.169.147.79._BAD_:1443/
- https://199.241.30.233._BAD_:449/
- https://151.248.123.100._BAD_:743/
- https://194.58.96.45._BAD_:4543/
- https://31.131.251.33._BAD_:743/
- https://62.210.214.106._BAD_:448/
- https://68.169.49.213._BAD_:448/

Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :

- ne pas ouvrir les documents ou les pièces jointes non sollicités ;
- 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.html

3 - Mise à jour mensuelle de Microsoft

Le 9 juin 2015, Microsoft a publié 8 bulletins de sécurité, dont 2 sont considérés comme critiques et 6 comme importants :

- MS15-056 (critique) qui concerne Internet Explorer ;
- MS15-057 (critique) qui concerne Windows Media Player ;
- MS15-059 (important) qui concerne Microsoft Office ;
- MS15-060 (important) qui concerne Microsoft Common Controls ;
- MS15-061 (important) qui concerne le noyau de Windows ;
- MS15-062 (important) qui concerne les services de fédération Active Directory ;
- MS15-063 (important) qui concerne le noyau de Windows ;
- MS15-064 (important) qui concerne Microsoft Exchange Server.

Internet Explorer

Microsoft, dans son dernier bulletin de sécurité (MS15-056), corrige 24 vulnérabilités au sein d'Internet Explorer. La majorité d'entre elles sont des vulnérabilités de type corruption de mémoire pouvant amener à une exécution de code arbitraire à distance. Elles sont exploitables sur toutes les versions du navigateur de la version 6 à la version 11.

Trois vulnérabilités de type élévations de privilèges (CVE-2015-1739, CVE-2015-1743, CVE-2015-1748) ont été corrigées et affectent les dernières versions d'Internet Explorer (jusqu'à la version 11).

Microsoft corrige une vulnérabilité (CVE-2015-1765) permettant l'accès à distance à l'historique de navigation de la victime. Cette dernière affecte les versions 9, 10 et 11 du navigateur.

Microsoft Office

Trois vulnérabilités résultant d'un mauvais traitement de format de fichier affectent les versions 2007, 2010 et 2013 de la suite bureautique. Ces défauts de sécurité peuvent provoquer une exécution de code arbitraire à distance.

Noyau de Windows

Onze vulnérabilités présentes dans plusieurs pilotes de Windows permettent l'élévation de privilèges et la fuite d'information. Elles affectent toutes les versions de Windows. Une de ces vulnérabilités affectant le pilote `win32k.sys` (CVE-2015-2360) a été utilisée lors d'une campagne d'attaque récente visant entre autres Kaspersky.

Une vulnérabilité affectant la fonction `LoadLibrary` exportée par la bibliothèque `kernel32.dll` ne valide pas correctement l'entrée utilisateur et de ce fait peut amener à une élévation de privilèges.

Documentation

- https://technet.microsoft.com/en-us/library/security/MS15-056
- https://technet.microsoft.com/en-us/library/security/MS15-057
- https://technet.microsoft.com/en-us/library/security/MS15-059
- https://technet.microsoft.com/en-us/library/security/MS15-060
- https://technet.microsoft.com/en-us/library/security/MS15-061
- https://technet.microsoft.com/en-us/library/security/MS15-062
- https://technet.microsoft.com/en-us/library/security/MS15-063
- https://technet.microsoft.com/en-us/library/security/MS15-064

4 - Rappel des avis émis

Dans la période du 08 au 14 juin 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-243 : Multiples vulnérabilités dans le noyau Linux Red Hat
- CERTFR-2015-AVI-244 : Multiples vulnérabilités dans Microsoft Internet Explorer

- CERTFR-2015-AVI-245 : Vulnérabilité dans Microsoft Windows Media Player
- CERTFR-2015-AVI-246 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-247 : Vulnérabilité dans Microsoft Common Controls
- CERTFR-2015-AVI-248 : Multiples vulnérabilités dans le noyau de Microsoft Windows
- CERTFR-2015-AVI-249 : Vulnérabilité dans Microsoft Active Directory Federation Services
- CERTFR-2015-AVI-250 : Vulnérabilité dans le noyau de Microsoft Windows
- CERTFR-2015-AVI-251 : Multiples vulnérabilités dans Microsoft Exchange Server
- CERTFR-2015-AVI-252 : Vulnérabilité dans QEMU
- CERTFR-2015-AVI-253 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-254 : Multiples vulnérabilités dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-255 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2015-AVI-256 : Vulnérabilité dans Cisco IOS XR
- CERTFR-2015-AVI-257 : Multiples vulnérabilités dans OpenSSL

Gestion détaillée du document

15 juin 2015 version initiale.