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 23 mars 2015
N° CERTFR-2015-ACT-012

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-012

1 - Avantages et limites d'Authenticode Windows

Problématique

Le système d'exploitation Windows, depuis Vista en 64 bits, impose que les pilotes de périphériques soient signés pour pouvoir être chargés.

Principe d'Authenticode

Signature de code

Le mode opératoire permettant de signer du contenu est le suivant :

- calculer un condensat du document que l'on veut signer ;
- chiffrer ce condensat avec la clef privée de l'émetteur ;
- transmettre le document avec le certificat (contenant la clé publique) et la signature, c'est-à-dire le résultat du chiffrement du condensat.

Ainsi, pour qu'une tierce personne vérifie le document, elle doit :

- calculer le condensat du document ;
- déchiffrer la signature au moyen de la clef publique présente dans le certificat ;
- vérifier que le condensat calculé est identique au condensat résultant du déchiffrement de la signature.

Afin de vérifier que le certificat utilisé pour la signature provient bien d'une entité de confiance, il doit y avoir un chaînage de certificats. Chaque certificat doit avoir signé le précédent et le dernier certificat de la chaîne doit être une autorité de confiance.

Authenticode

Authenticode a été initialement introduit pour la vérification des contrôles ActiveX sous Internet Explorer, la version 2.0 d'Authenticode arrivant sous Internet Explorer 3.

Authenticode est aujourd'hui disponible pour signer les types de fichiers suivants :

- "*.cab" ;
- "*.cat" ;
- "*.ctl" ;
- "*.dll" ;
- "*.exe" ;
- "*.ocx" ;
- "*.sys".

Le procédé de signature suit le mode opératoire décrit précédemment et calcule le « PEHash » du binaire.

Il s'agit du condensat du binaire sans tenir compte du code de redondance cyclique (CRC) (puisque celui-ci sera calculé une fois la signature ajoutée au binaire) ni des informations relatives au bloc contenant la signature Authenticode (celles-ci seront complétées une fois le processus de signature effectué).

Ce condensat peut être calculé avec les fonctions de hashage MD5, SHA-1 (à partir de Windows Vista) ou SHA-256 (à partir de Windows 8).

La liste des autorités de confiance d'un système Windows correspond au magasin de certificats « Autorités de certification racine de confiance ».

Limitations de la signature de code

Utilisation détournée

Le bulletin d'actualité CERTFR-2015-ACT-008 présentait la technique de substitution de bibliothèque.

Cette technique ne modifie pas le code du binaire signé, mais seulement le code issu de bibliothèques non signées que le binaire est amené à charger. Aucune alerte n'est levée car le binaire exécuté est correctement signé. La bibliothèque n'étant pas signée, il n'y a aucun moyen pour le système de vérifier l'intégrité de son code.

C'est une méthode très largement utilisée par le programme malveillant PlugX pour s'installer sur un système sans alerter l'utilisateur.

Vol de clef privée

Si un éditeur de logiciel peut signer son code, toute personne disposant de la clef privée et du mot de passe associé pourra également signer du code au nom de cet éditeur. Le cas s'est notamment présenté lors de la compromission de Sony Pictures Entertainment, où des clefs privées de certificats de signature de code ont été exfiltrées par les attaquants. Ces derniers ont ainsi pu produire des codes malveillants de la famille Destover, signés avec un certificat provenant de Sony.

Pour s'assurer que les secrets cryptographiques ne sont pas détournés, il conviendra de sensibiliser les personnels amenés à les manipuler et de mettre en place un réseau et un environnement dédiés et isolés.

Code vulnérable

Les éditeurs de logiciels ne sont pas à l'abri de potentielles vulnérabilités dans leurs produits. Le cas critique est celui des pilotes de périphériques, dont le code s'exécute en espace noyau, dans le cas où des vulnérabilités de type élévation de privilèges sont exploitables. Ces pilotes vulnérables n'en restent pas moins numériquement signés et donc jugés de confiance conformément à la politique de sécurité du système d'exploitation.

Cette méthode pour exécuter du code en espace noyau a notamment été utilisée par le maliciel « Uroburos ». Il utilise en effet un ancien pilote de périphérique VirtualBox, vulnérable, pour exécuter du code privilégié. Les acteurs du groupe « Equation » ont également eu recours à un ancien pilote de périphérique de CloneCD de la société Elaborate Bytes pour effectuer un changement de la politique de sécurité du système afin d'autoriser le chargement de pilotes de périphériques non signés.

Documentation

– Bulletin d'actualité CERTFR-2015-ACT-008 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-008/

2 - Mise à jour de l'outil EMET

Présentation et finalités d'EMET

EMET (« Enhanced Mitigation Experience Toolkit ») est une trousse à outils de Microsoft destinée à empêcher l'exploitation de vulnérabilités logicielles.

EMET met en oeuvre des protections spécifiques que d'éventuels attaquants devront successivement mettre en échec pour tenter de compromettre un poste Windows. Il peut être déployé sur toutes les versions du système d'exploitation de Microsoft (postes clients ou serveurs) depuis Windows Vista. Il permet également de sécuriser

des logiciels tiers (Mozilla Firefox, Google Chrome, Winzip, VLC, etc.). Simple à configurer, notamment grâce à des profils prédéfinis, il peut être utilisé par des particuliers ou déployé sur un parc informatique d'entreprise.

EMET dispose de fonctionnalités de journalisation très utiles pour identifier des risques de sécurité avérés (applications faillibles, certificats SSL suspects, etc.). Munis de ces informations, les administrateurs pourront prendre les mesures correctrices nécessaires comme la mise à jour des applications ou le durcissement d'une configuration.

Les enregistrements générés par EMET (dont le event source est « EMET ») sont stockés au sein du journal des Applications (fichier AppEvent.Evt ou Application.evtx). Les événements de type « Information » concernent l'activité normale d'EMET, comme par exemple le lancement de l'Agent EMET. Les événements de type « Warning » concernent les changements de la configuration d'EMET ou certains messages liés à la validation de certificats SSL. Les événements de type « Error » sont les plus intéressants. Ils sont générés lorsqu'EMET bloque une tentative d'exploitation d'une faille applicative ou identifie un certificat SSL suspect. Les événements de ce type font également l'objet d'un message spécifique adressé directement à l'utilisateur, via la zone de notification de la barre des tâches.

Sortie de EMET 5.2

Le 16 mars 2015, Microsoft a publié la version 5.2 d'EMET. Cette version introduit de nouvelles fonctionnalités :

- Control Flow Guard : la bibliothèque « EMET.DLL » est compilée avec le *Control Flow Guard* (CFG) activé. Cette nouvelle fonctionnalité supportée par Windows 8.1 et Windows 10 permet de valider le chemin d'exécution d'une application. Elle prévient les tentatives d'exécutions partielles du code, souvent utilisées dans le cadre d'exploitation par *Return Oriented Programming* (ROP);
- VBScript in Attack Surface Reduction : EMET a configuré son *Attack Surface Reduction* (ASR) pour prévenir des exécutions de code VBScript. Le VBScript est souvent utilisé pour l'exploitation de vulnérabilités appelée « VBScript God Mode » sur le navigateur *Internet Explorer* ;
- Enhanced Protected Mode/Modern IE : EMET supporte maintenant totalement le mode *Enhanced Protected Mode* d'*Internet Explorer*. Ce mode permet un renforcement global de la sécurité du navigateur.

Conclusion et recommandations

Si le risque de contournement des mesures de protection déployées par EMET ne peut être écarté, il demeure un moyen simple et efficace de durcir un système. Le CERT-FR recommande l'intégration de cet utilitaire dans les systèmes d'information, dès que possible. Il reste cependant pertinent de qualifier cette intégration avant tout déploiement d'ampleur, afin d'éviter d'éventuels effets de bord sur les applications métier.

Si EMET peut contribuer à durcir la sécurité d'un système, il n'en demeure pas moins que les mesures recommandées dans le guide d'hygiène informatique doivent être appliquées consciencieusement. L'ensemble des systèmes d'exploitation et des logiciels utilisés sur un parc informatique doivent être cartographiés et maintenus à jour selon une politique de mise à jour clairement définie en suivant les publications de vulnérabilités des différents éditeurs et en appliquant les correctifs au plus tôt.

Documentation

- Présentation de la trousse à outils EMET par Microsoft :
  http://support.microsoft.com/kb/2458544/fr
- Téléchargement d'EMET :
  http://www.microsoft.com/emet
- Présentation d'EMET 5.2 par Microsoft :
  http://blogs.technet.com/b/srd/archive/2015/03/12/emet-5-2-is-available.aspx
- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3 - Rappel des avis émis

Dans la période du 16 au 22 mars 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-115 : Multiples vulnérabilités dans Moodle

– CERTFR-2015-AVI-116 : Multiples vulnérabilités dans Drupal
– CERTFR-2015-AVI-117 : Multiples vulnérabilités dans OpenSSL
– CERTFR-2015-AVI-118 : Multiples vulnérabilités dans Mac OS X Yosemite

Gestion détaillée du document

23 mars 2015 version initiale.