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 07 mars 2014
N° CERTFR-2014-ACT-010

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-010

1 - Compromission de serveurs afin de générer des "Bitcoin"

Les motivations d'un attaquant pour compromettre un système peuvent être multiples : le sabotage (destruction d'information, blocage de services, etc.), la revendication politique ou idéologique (défiguration de site Web, etc.), l'espionnage (compromission de réseaux transmettant des informations sensibles, etc.) ou l'appât d'un gain financier.

Dans ce dernier cas, un attaquant cherche généralement à compromettre un grand nombre de machines et à les intégrer dans un réseau (ou botnet) dont il a le contrôle. Il peut alors louer les ressources informatiques de ce réseau, par machine et par unité de temps pour diverses opérations telles que l'envoi de courriels non sollicités (spam) ou la réalisation d'attaques en déni de service.

Depuis quelques mois, il est également devenu profitable pour un attaquant d'utiliser de telles ressources pour générer à son profit des monnaies virtuelles, la plus populaire étant le « Bitcoin ». Ainsi, le CERT-FR a été amené à traiter des compromissions de serveurs où l'attaquant avait déposé des outils de calcul intensif, très consommateurs en ressources processeur, afin de générer certaines de ces monnaies virtuelles.

Généralement utilisée à des fins de suivi de la qualité de service, la supervision de la charge processeur d'un serveur permet de détecter une activité malveillante intensive sur un système compromis (envoi continu de courriels non sollicités, calcul de monnaie virtuelle, cassage de mots de passe, etc.).

Lorsque cela est envisageable et pertinent, le CERT-FR recommande d'intégrer cet indicateur dans la supervision des systèmes afin de détecter ce type d'incident.

2 - EMET et la prévention d'exploitation de vulnérabilités

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 XP. Outre les applications Microsoft 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 car 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 feront également l'objet d'un message spécifique adressé directement à l'utilisateur via la zone de notification de la barre des tâches.

Tableau 1 - Identifiants d'événements (EventId) générés par EMET version 3.0/4.0 :

EMET	3.0/4.0
Information	00
Warning	01
Error	02

Tableau 2 - Identifiants d'événements (EventId) générés par EMET Version 4.1 :

	EMET Mitigation,	EMET GUI,	EMET Command Line,	EMET Agent,	Certificate Trust
Information	00,	10,	20,	30,	40
Warning	01,	11,	21,	31,	41
Error	02,	12,	22,	32,	42

Sortie de EMET 5.0 Technical Preview

Le 25 février 2014, Microsoft a publié la version 5.0 de EMET en « *Technical Preview* ». Cette version introduit de nouvelles fonctionnalités qui seront finalisées dans la prochaine version stable. Il est important de signaler que Microsoft propose ce produit non finalisé afin d'obtenir des retours de la part des utilisateurs. Il est également précisé que cette version doit être utilisée dans un environnement de test.

Deux améliorations sont particulièrement visibles. Elles reposent sur l'ajout de fonctionnalités « *Attack Surface Reduction* » (ASR) et « *Export Address Table Filtering Plus* » (EAF+). De nouvelles techniques d'identification d'exploitation de vulnérabilités par « *Return Oriented Programming* » (ROP) ont également étés ajoutées. La fonctionnalité ASR permet de bloquer le chargement de certains modules ou greffons spécifiques depuis une application. Par exemple, il est possible de configurer EMET pour empêcher le chargement du greffon Adobe Flash Player depuis Microsoft Word ou de bloquer l'exécution d'appliquettes Java depuis Internet Explorer sur la zone de sécurité Internet tout en continuant à autoriser l'exécution de celles-ci sur la zone Intranet.

La fonctionnalité EAF est utilisée pour contrôler les accès en lecture aux tables d'export (« *Export Address Table* » ou EAT) de certaines bibliothèques sensibles (`kernel32.dll` et `ntdll.dll`). Pour cela, cette protection positionne des points d'arrêt matériel aux adresses mémoires correspondant à ces tables d'export, les accès en lecture à ces dernières étant alors contrôlés par un gestionnaire d'exception. L'objectif de cette protection est de bloquer l'exécution de certains codes malveillants qui recherchent en mémoire ces tables d'export pour construire dynamiquement des gadgets utilisés dans des chaînes ROP ou pour identifier les adresses de certaines fonctions spécifiques.

EAF+ améliore la protection EAF déjà présente dans les versions antérieures en ajoutant notamment la protection de la bibliothèque kernelbase.dll et en renforcant l'identification d'appels illégitimes.

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. La version 5.0 d'EMET étant pour l'instant disponible uniquement en version de test, le CERT-FR ne recommande pas sa mise en oeuvre dans un système en production. Il peut cependant être pertinent de le déployer sur un environnement de test afin de qualifier son impact sur les applications métier et ainsi d'anticiper un déploiement élargi sur l'ensemble du parc.

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 scrupuleusement les publications de vulnérabilités des différents éditeurs et des sites des CERT 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://technet.microsoft.com/en-us/security/jj653751
- Présentation d'EMET 5.0 par Microsoft :
  http://blogs.technet.com/b/srd/archive/2014/02/25/announcing-emet-5-0-technical-preview.aspx
- Bulletin d'actualité 2013-25 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-025/
- Bulletin d'actualité 2013-03 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-003/
- Bulletin d'actualité 2009-44 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2009-ACT-044/
- 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 28 février au 06 mars 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-095 : Multiples vulnérabilités dans Apple OS X
- CERTFR-2014-AVI-096 : Vulnérabilité dans IBM Rational Tester
- CERTFR-2014-AVI-097 : Vulnérabilité dans GnuTLS
- CERTFR-2014-AVI-098 : Vulnérabilité dans Novell ZENworks
- CERTFR-2014-AVI-099 : Vulnérabilité dans EMC RSA
- CERTFR-2014-AVI-100 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-101 : Multiples vulnérabilités dans Cisco Wireless LAN Controller
- CERTFR-2014-AVI-102 : Vulnérabilité dans Cisco Wireless-N VPN
- CERTFR-2014-AVI-103 : Multiples vulnérabilités dans Puppet
- CERTFR-2014-AVI-104-001 : Vulnérabilité dans Nginx
- CERTFR-2014-AVI-105 : Multiples vulnérabilités dans Citrix NetScaler
- CERTFR-2014-AVI-106 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

07 mars 2014 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-010`