

SEPTEMBRE 2003

## Système d'activation des produits Macromedia

Macromedia a mis en place un nouveau système d'activation dans Contribute 2 et ses produits MX 2004 : Studio, Dreamweaver, Flash, Fireworks et FreeHand. Macromedia fournit une bonne documentation de ce système et de l'objectif de sa mise en place, de même que des détails techniques. @stake a analysé ce système afin de vérifier qu'il protège bien les informations échangées entre ces produits et le serveur d'activation de Macromedia.

### Vue d'ensemble

Le système d'activation a été conçu pour vérifier la validité de la licence d'un produit, afin de permettre l'utilisation de ce dernier. Alors que cette technique de validation est utilisée par de nombreux éditeurs de logiciels afin d'assurer le respect des clauses du contrat de licence, c'est la première fois qu'elle est utilisée par Macromedia.

Macromedia comprend bien l'importance d'une telle fonction, mais aussi la crainte qu'elle peut inspirer quant aux informations divulguées, et a donc décidé d'en expliquer le fonctionnement. Macromedia a demandé à @stake de fournir une opinion indépendante et de vérifier le respect de l'anonymat et de la protection des informations échangées entre l'utilisateur et Macromedia.

Il est important de noter que @stake a reçu la version finale du logiciel. @stake a téléchargé et installé le logiciel en suivant le processus que tout autre utilisateur final doit suivre. Les versions Mac OS X et Windows ont été évaluées avec différentes configurations. Pendant l'installation et l'activation, @stake a vérifié que le comportement du logiciel correspondait à la documentation fournie par Macromedia.

@stake a pris en compte un certain nombre de points soulevés par Macromedia. Dans chaque cas, @stake a pu confirmer la validité des promesses faites par Macromedia, et le respect des pratiques courantes au sein de l'industrie informatique.

**Promesse 1 : le système d'activation via Internet ne recueille ou ne transmet aucune information qui pourrait permettre d'identifier l'utilisateur.**

@stake a vérifié ce point en identifiant la source de toutes les informations échangées entre chaque application Macromedia et le serveur d'activation de Macromedia.

Les tests menés par @stake ont confirmé la simplicité du processus d'activation : l'ensemble des communications requises pour l'activation consiste en une seule requête émise par le client et en une seule réponse renvoyée par le serveur d'activation de Macromedia. L'étude des informations échangées a donc été grandement simplifiée.

L'exemple A montre une requête complète capturée et déchiffrée à l'aide de WebProxy 2 [1].

---

**Exemple A : requête d'activation**

--->>--- \*\* https\_3 \*\* Client request to activate.macromedia.com:443 (secure) (04:00:25/11-Jul-2003) --->>---

POST /\_macromedialicensing/cgi-bin/go.cgi/webstore/XMLActivation HTTP/1.0

User-Agent: MMxpt

Host: activate.macromedia.com

Content-Length: 533

Cache-Control: no-cache

Connection: close

XML=<?xml version='1.0' encoding='UTF-8' ?>

<LicenseRequest Version='2.0' ClientVersion='3.0.0.105,241000,9.0' LicenseType='SafeCast'

Locking='NodeLock'>

<LicenseFulfillment Type='New'>

<ProductLicenseID>2986577920</ProductLicenseID>

<ProductBuildID>Contribute, en, 2.0, Win</ProductBuildID>

<ReportingDetail>Windows 2000, ENU, 5.0.2195</ReportingDetail>

<ActivationCode>CTD200-79355-97216-90420</ActivationCode>

<ClientData>7322550213856595219531635531509565870998198650962954287203290906</ClientData>

</LicenseFulfillment>

</LicenseRequest>

---

Cet exemple montre clairement que la plus grande partie du contenu ne pose aucun risque d'atteinte à la sécurité des informations :

- L'en-tête POST est au format standard, sans informations spécifiques concernant le client.
- Les données XML ClientVersion, ProductLicenseID et ProductBuildID ne correspondent qu'aux informations concernant le logiciel objet de l'activation.
- Comme indiqué par Macromedia, le nom, la version et la langue du système d'exploitation sont indiqués dans ReportingDetail.
- Le code d'activation est le numéro de série fourni lors de l'achat du produit.

Le champ ClientData présente un défi un peu plus important, étant donné que son contenu n'est pas tout de suite évident. @stake a donc dû décompiler le logiciel fourni par Macromedia afin de déterminer l'origine des données ClientData. Le code utilisé pour produire les données ClientData est masqué, de façon à ne pas en permettre l'examen. @stake a cependant réussi à isoler

quelques-unes des routines de base. Les informations utilisées pour produire les données ClientData sont, entre autres, le nombre de battements du processeur, l'heure système, l'heure locale, l'identifiant de processus et l'identifiant de tâche. Certaines variantes existent entre les applications testées et @stake n'a pas pu identifier toutes les informations utilisées pour les données ClientID. La production des données ClientData à plusieurs reprises sur le même ordinateur n'a pas permis à @stake de détecter de structure particulière au niveau des valeurs utilisées.

La collection de valeurs est combinée à l'aide d'algorithmes de chiffrement, la valeur finale étant représentée sous une forme décimale. Les tests effectués par @stake n'ont pas permis de détecter l'inclusion d'informations qui pourraient permettre d'identifier l'utilisateur.

---

#### Exemple B : réponse du serveur d'activation

```

---<<<--- ** https_3 ** Server response from activate.macromedia.com:443 (secure) ---<<<---

HTTP/1.1 200 OK
Date: Fri, 11 Jul 2003 10:58:03 GMT
Server: Apache/1.3.23 (Unix) mod_perl/1.26 mod_ssl/2.8.7 OpenSSL/0.9.6c
Set-Cookie:
MACROMEDIA LICENSING_PREFS=1.2%3ACOO KIE_VER52616e646f6d4956f52730b1efe42e4d75db346304
1d586b18ab36c80f2f0f8203e5092671a65bc93ea2eacf554dae571946669c917a8de671a2d3814283d9c;
domain=.releasesoftware.com; path=/; expires=Wed, 09 Jul 2008 10:58:17 GMT
Set-Cookie: RELEASE_SESSION=192.168.0.10.94751057921083579; path=/
Content-length: 695
Connection: close
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<LicenseRequest Version="2.0" ClientVersion="3.0.0.105,241000,9.0" LicenseType="SafeCast"
Locking="NodeLock">
<LicenseFulfillment Type="New">
<ProductLicenseID>2986577920</ProductLicenseID>
<ProductBuildID>Contribute, en, 2.0, Win</ProductBuildID>
<ReportingDetail>Windows 2000, ENU, 5.0.2195</ReportingDetail>
<ActivationCode>CTD200-79355-97216-90420</ActivationCode>
<ClientData>7322550213856595219531635531509565870998198650962954287203290906</ClientData>
<License>2152 8485 9710 0355 0403 6067 2522 0111 0181 5323 1032 5129 1591 2255 7921 2125 7286 4571
4013 8035 3211 1227 0746 3794 0518 0693</License>
</LicenseFulfillment>
</LicenseRequest>
<!-- Complete -->

```

---

Les tests effectués par @stake confirment donc que la requête envoyée pour demander l'activation ne contient pas d'informations qui pourraient permettre d'identifier l'utilisateur.

Alors que les risques sont moindres pour les données renvoyées à un produit Macromedia par le serveur d'activation, il peut être bon d'examiner cette réponse d'un peu plus près.

L'exemple B montre la réponse du serveur d'activation, telle qu'enregistrée par WebProxy, à la suite de la requête illustrée par l'exemple A. Le contenu de la réponse est identique à celui de la requête, à une différence près. Le contenu XML comprend maintenant une valeur « License », ce qui n'a rien d'étonnant.

**Promesse 2 : toutes les informations échangées dans le cadre du processus d'activation sont protégées avec SSL.**

@stake a surveillé toutes les communications réseau émanant du logiciel Macromedia au cours de l'installation et de l'activation du produit. Toutes les données échangées au cours du processus d'activation sont chiffrées avec SSLv2-TLS, la meilleure méthode de chiffrement des transactions web, comme le mentionne Macromedia dans sa documentation.

Sous Windows, le système d'activation mis en place par Macromedia utilise la bibliothèque wininet.dll pour le transfert des données. Cette bibliothèque est distribuée avec le système d'exploitation et est utilisée par d'autres programmes, tel qu'Internet Explorer. Cela permet d'assurer une implémentation correcte et d'assurer que des paramètres de configuration uniques, tels qu'un proxy ou un pare-feu, sont parfaitement acceptés.

Les requêtes et les réponses transmises au cours du processus d'activation sont échangées à l'aide d'une méthode de chiffrement standard, comme Macromedia l'a indiqué dans sa documentation.

.....  
**Exemple C : requête de transfert de licence**  
 .....

--->>--- \*\* https\_5 \*\* Client request to activate.macromedia.com:443 (secure) (05:03:42/11-Jul-2003) --->>---

```
POST /_macromedialicensing/cgi-bin/go.cgi/webstore/XMLActivation HTTP/1.0
User-Agent: MMxpt
Host: activate.macromedia.com
Content-Length: 538
Cache-Control: no-cache
Connection: close
```

```
XML=<?xml version='1.0' encoding='UTF-8' ?>
<LicenseRequest Version='2.0' ClientVersion='3.0.0.105,241000,9.0' LicenseType='SafeCast'
Locking='NodeLock'>
<LicenseFulfillment Type='Giveback'>
<ProductLicenseID>2986577920</ProductLicenseID>
<ProductBuildID>Contribute, en, 2.0, Win</ProductBuildID>
<ReportingDetail>Windows 2000, ENU, 5.0.2195</ReportingDetail>
<ActivationCode>CTD200-79355-97216-90420</ActivationCode>
<ClientData>2093748477214062099566593896266237971887305918513664114680315762</ClientData>
</LicenseFulfillment>
</LicenseRequest>
```

.....

**Promesse 3 : le mécanisme de transfert de licence ne recueille ou ne transmet aucune information qui pourrait permettre d'identifier l'utilisateur.**

Le mécanisme de transfert de licence oblige à une communication entre les produits Macromedia et le serveur d'activation de Macromedia. Il pourrait donc, en tant que tel, présenter un risque.

Là encore, la simplicité du mécanisme de transfert de licence permet de vérifier les informations échangées. Le transfert de licence effectué par @stake a permis de constater que la seule communication entre chaque produit Macromedia et le serveur d'activation de Macromedia est la requête illustrée dans l'exemple C.

La seule différence entre cette requête et la réponse est que « LicenseFulfillment » est de type « Giveback ».

Les tests effectués par @stake confirment donc que la requête de transfert de licence ne conduit pas à l'échange d'informations qui pourraient permettre d'identifier l'utilisateur.

**Promesse 4 : le système d'activation par téléphone ne recueille ou ne transmet aucune information qui pourrait permettre d'identifier l'utilisateur.**

Les applications Macromedia peuvent également être activées par téléphone. Le processus d'activation par téléphone utilise un sous-ensemble des informations transmises au cours de l'activation par Internet. Les données de l'exemple D sont utilisées pour créer une requête d'activation par téléphone.

**Exemple D : exemple de requête d'activation par téléphone**

|  |                                      |
|--|--------------------------------------|
| 02 19 03 200 7 9355 97216 90420        | -- code d'activation                 |
| 21659 38036 12799 42445 35604 98157 51 | -- 32 chiffres de données de client  |
| 10000140 02                            | -- 10 chiffres de données de version |

Bien que le code d'activation soit d'une forme quelque peu différente, les lettres A-Z ont été remplacées par les chiffres 0-25 de façon à faciliter la saisie sur un clavier de téléphone, ce qui ne conduit toujours pas à l'échange d'informations présentant des risques. De même, les informations concernant la version ne présentent aucun risque.

@stake a dû, afin de vérifier le contenu des 32 autres chiffres de la requête, décompiler les fichiers binaires fournis par Macromedia de façon à identifier la source des données. Cette source est la même que celle utilisée pour produire les données nécessaires à l'activation par Internet. Le nombre de battements du processeur, l'heure système, l'heure locale, l'identifiant de processus et l'identifiant de tâche n'étant pas des données uniques, ces informations ne présentent pas de risque particulier.

**Promesse 5 : le gestionnaire de licence n'est exécuté qu'en même temps que les applications Macromedia, n'utilise qu'une quantité réduite de ressources, et est désinstallé en même temps que les applications Macromedia.**

Le mécanisme de vérification de la licence à l'exécution est implémenté, sur les plates-formes Macintosh et Windows, sous forme de service exécuté en même temps que les applications Macromedia. @stake a surveillé le comportement du gestionnaire de licence : alors que ce comportement est similaire sur les deux systèmes d'exploitation, sa forme diffère quelque peu.

Les deux plates-formes utilisent plusieurs fichiers de données et des clés de registre contenant des informations binaires représentant la licence. Bien que ces conteneurs de données soient utilisés de façon répétée au cours de l'exécution, leur utilisation et leur structure ne permettent pas de conclure qu'ils contiennent des contenus exécutables.

Sur Mac OS X, un fichier binaire SUID appelé « Authentication Service » est exécuté à plusieurs reprises au démarrage d'une application Macromedia. L'exécution du service d'authentification continue une fois l'application Macromedia correctement initialisée, et ne se termine qu'en même temps que l'application Macromedia.

Sous Windows 2000/XP, le gestionnaire de licence est installé sous forme de service en démarrage manuel et est appelé « Macromedia Licensing Service ». Un processus supplémentaire, « ~e5d141.tmp », lié au gestionnaire de licence, existe également. Deux instances de ce processus au nom étrange peuvent être détectées pendant l'exécution de l'application Macromedia.

Quelques fichiers temporaires contenant des bibliothèques de code utilisées par l'application Macromedia et le gestionnaire de licence sont également créés au cours de l'exécution. Ces fichiers temporaires portent un nom dynamique, affecté au début de l'exécution de l'application Macromedia, et sont supprimés à la fermeture de l'application.

@stake a vérifié que l'arrêt de l'application Macromedia entraîne également l'arrêt du gestionnaire de licence et la suppression des fichiers temporaires. De plus, la désinstallation de l'application Macromedia entraîne la suppression du gestionnaire de licence.

Les tests réalisés par @stake ont permis de valider la description fournie par Macromedia.

### **Conclusion**

Les tests réalisés par @stake et l'examen des fichiers binaires de Contribute 2 et des applications Macromedia nous ont permis de confirmer la validité des informations fournies par Macromedia quant au fonctionnement de son système d'activation. Macromedia a réussi à réduire la quantité d'informations échangées au cours du processus d'activation de façon à éliminer le risque de transfert d'informations permettant d'identifier l'utilisateur.

**A propos de @stake, Inc.**

@stake, Inc., offre des services et produits conçus pour évaluer et gérer les risques présentés par les environnements informatiques en place dans les entreprises. Nos services SmartRisk couvrent les principaux aspects liés à la sécurité, pour les applications, les infrastructures, les réseaux avec ou sans fil, les systèmes de stockage, la formation et la réponse aux incidents. Nos ingénieurs-conseils combinent expertise technique et connaissances commerciales pour créer des solutions complètes destinées à protéger votre entreprise. Première entreprise à avoir développé un modèle empirique permettant de mesurer le retour sur investissement en mesures de sécurité, @stake produit des solutions répondant parfaitement aux besoins en sécurité des entreprises. Basée à Cambridge (Massachusetts), @stake dispose de bureaux à Londres, New York, Raleigh (Caroline du Nord), San Francisco (Californie) et Seattle (Washington). Consultez [www.atstake.com](http://www.atstake.com) pour obtenir de plus amples informations.

---

**Notes et références**

[1]WebProxy est un outil de sécurité interactif conçu pour tester la sécurité des applications web. Consultez <http://www.atstake.com/webproxy> pour obtenir de plus amples informations.

@stake a intercepté et déchiffré les communications réseau HTTP et HTTPS avec Internet Explorer (et wininet). WebProxy ne disposant pas des autorisations nécessaires pour accéder au site d'activation de Macromedia, le processus d'activation n'a pas pu, initialement, aboutir. @stake a donc configuré wininet pour une utilisation du certificat autosigné de WebProxy. Une fois cette configuration établie, les informations d'activation ont pu être déchiffrées par WebProxy, avant d'être chiffrées une nouvelle fois avant leur renvoi au serveur d'activation.

@stake utilise fréquemment ce type de test avec les applications web sécurisées. L'accès aux données déchiffrées obligeant le client à ajouter un certificat de confiance pour WebProxy, les contenus XML déchiffrés ne seraient pas visibles dans un environnement normal.