

Objet : Grande propagation d'une famille de vers destructifs appelée **Areses** qui utilise son propre moteur de SMTP pour se reproduire en envoyant une copie de lui même à toutes les adresses collectées de la machine victime.

Alias: [Win32/]Areses Family; [VBS/]Areses!generic; [W32.]Areses.A@mm; [Email-Worm.]Win32.Bagle.fw; [Win32.]Areses ;

Systèmes concernés : Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

Effets	<p>Lorsque le ver Areses s'exécute, il tente de :</p> <ol style="list-style-type: none">1- Se copier dans le répertoire d'installation de Windows sous le nom de csrss.exe2-Remplacer le programme de débogage en modifiant la valeur : "Debugger" = "[PATH TO WORM]" au niveau de la clé HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\explorer.exe3- Ajouter la valeur "Application" = "[FF FA 6E 06]" au niveau de la clé HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Devices4.Injecter son code dans les processus svchost.exe et services.exe.5.Collecter toutes les adresses email à partir des fichiers ayant les extensions suivantes : .adb, .asp, .cfg, .cgi, .dbx, .dhtm, .eml, .htm, .html, .jsp, .mbx, .mdx, .mht, .mmf, .msg, .nch, .ods, .oft, .php, .pl, .sht, .shtml, .stm, .tbb, .txt, .uin, .wab, .wsh, .xls, .xml, .dhtml6.Chercher la chaîne 127.0.0.1 au niveau de la clé: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interface\{INTERFACE CLSID}"NameServer" Une fois trouvée, le ver arrête son moteur de SMTP.7.Se cacher dans une archive qui porte la nom message.zip dans le dossier temporaire de Windows8.Ouvrir une porte dérobée avec un port TCP aléatoire
Signes visibles d'infection	<p>- Le moteur utilise son propre moteur de SMTP pour envoyer une copie de lui même aux adresses collectées, l'adresse de l'expéditeur est spoofée, le sujet, le message et la pièce jointe sont aléatoires.</p> <p>- Le ver essaie de se connecter aux adresses suivantes :</p> <p>[http://85.249.23.35/m/][Blocked]</p> <p>[http://207.46.250.119/g/][Blocked]</p> <p>[http://84.22.161.192/s/][Blocked]</p> <p>Il peut également ouvrir Internet Explorer et se connecter au site http://www.nahuy.com</p>
Degré d'infection à l'échelle Internationale	moyennement élevé (Niveau 3)
Degré d'infection à l'échelle nationale	Limité
Propagation	via courrier électronique
Pour plus de détails	<p>http://ivic.zonelabs.com/tmpl/body/CA/virusDetails.jsp?VId=53737 http://fr.mcafee.com/virusInfo/default.asp?id=description&virus_k=139209 http://www.sarc.com/avcenter/venc/data/w32.areses.h@mm.html</p>

Solution

Mesures préventives

Il est toujours conseillé de prendre les mesures préventives suivantes :

- Ne pas ouvrir des fichiers joints de messages aux quels vous ne vous attendez pas.
- Isoler immédiatement les machines infectées pour empêcher une plus ample propagation au sein de votre réseau.
- Configurer votre serveur mail de sorte à bloquer ou de supprimer tout email ayant des fichiers joints communément utilisés pour la propagation de virus

Désinfection

Si vous pensez avoir été infecté, il faudra ainsi :

- Désactiver l'option Restauration du système (Windows Me/XP).
- Au cas où vous avez un anti-virus :
 - mettre à jour la base de signature de votre antivirus.
 - Effectuer un scan complet du système et supprimer tous les fichiers infectés.
 - Supprimer toutes les valeurs ajoutées au registre.
- Au cas où vous n'avez pas installé un antivirus et si vous êtes un utilisateur domestique, vous pouvez installer gratuitement l'un des anti-virus proposés par l'Agence.