G-Data : Exploitation des failles de Java
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 8/11/2010 11:30:00

Le classement des dangers pour le mois dâ□□octobre rÃ©alisÃ© par **G Data Software AG**, fait apparaÃ®tre en premiÃ¨re position **un malware exploitant une vulnÃ©rabilitÃ© Java**.

Cette arrivÃ©e rapide de ce malware apparu seulement au dÃ©but du mois dâ□□octobre conduit lâ□□Ã©diteur Ã alerter tous les utilisateurs sur lâ□□urgence de mise Ã jour de leur lecteur Java et de toutes les applications exploitant ce langage de programmation.

Alors que depuis plusieurs mois les malwares exploitant les vulnÃ©rabilitÃ©s des fichiers PDF dominaient le top 10, un nouvel entrant, Java.Trojan.Exploit.Bytverify qui exploite les vulnÃ©rabilitÃ©s dans Java, arrive en tÃªte des malwares du mois dâ□□octobre.

Lâ□□exploitation des vulnÃ©rabilitÃ©s dans des logiciels constitue actuellement la faÃ§on la plus efficace dâ□□infecter en nombre des ordinateurs afin dâ□□en prendre le contrÃ´le. Le mode dâ□□infection du malware Java.Trojan.Exploit.Bytverify.N se rÃ©alise par Â« drive by download Â», autrement dit il suffit dâ□□ouvrir une page Internet infectÃ©e pour Ãªtre contaminÃ©.

Le top 5 commentÃ© et les conseils pour se protÃ©ger :

1Ã¨re place : Java.Trojan.Exploit.Bytverify.N

Ce type de malware exploite une faille de sÃ©curitÃ© dans le vÃ©rificateur de code de Java. Il peut se trouver dans les applets Java des sites Web. Lâ□□utilisation de cet exploit permet l'exÃ©cution du code malveillant. Il peut alors tÃ©lÃ©charger, par exemple, un cheval de Troie. Un cybercriminel

peut ainsi gagner le contrÃ´le du systÃ¨me de la victime.

La mise Ã jour des applications Java de lâ□□ordinateur et lâ□□installation dâ□□un antivirus intÃ©grant un scan HTTP sont des conditions primordiales.

2e place : Worm.Autorun.VHG

Ce vers exploitant lâ□□Autorun de Windows se diffuse Ã partir de clÃ© USB ou de disques durs externes.

Avant de transfÃ©rer sur votre ordinateur des donnÃ©es provenant de supports de stockage externes, faites un scan antivirus des donnÃ©es.

Malware in October 2010

	Name	Percentage	Trend*
1	Java.Trojan.Exploit.Bytverify.N	2,12 %	new
2	Worm.Autorun.VHG	1,32 %	↔
3	JS:Pdfka-OE [Expl]	1,14 %	↘
4	WMA:Wimad [Drp]	1,05 %	↘
5	Application.Keygen.BI	0,87 %	↗
6	Win32:Enistery [Susp]	0,85 %	new
7	JS:Downloader-AEY [Trj]	0,67 %	new
8	Win32.Sality.OG	0,51 %	↗
9	JS:Downloader-AFR [Trj]	0,42 %	new
10	JS:Downloader-AEU [Trj]	0,36 %	new

3 e place : JS:Pdfka-OE [Expl]

Ce malware tire avantage des vulnÃ©rabilitÃ©s JavaScript dans les programmes PDF. Il suffit dâ□□ouvrir un fichier PDF infectÃ© pour que le cybercriminel accÃ¨de Ã lâ□□ordinateur de sa victime.

Nâ□□ouvrez pas les fichiers provenant de destinataires inconnus ou ceux issus de chaÃ®nes de diffusion

4 e place : WMA:Wimad [Drp]

Cet injecteur de cheval de Troie se prÃ©tend comme un fichier audio WMA lÃ©gitime et invite

lâ□□utilisateur Ã installer un Codec vidÃ©o. Ã□ dÃ©faut de vidÃ©o lâ□□infection est bien prÃ©sente.

Lorsque vous souhaitez visionner une vidÃ©o (gÃ©nÃ©ralement dâ□□actualitÃ©) sur un site que vous dÃ©couvrez pour la premiÃ¨re fois (souvent en langue anglaise) nâ□□acceptez aucun tÃ©lÃ©chargement de codec.

5 e place : Application.Keygen.BI

Ce malware se cache dans les gÃ©nÃ©rateurs de clÃ© disponibles sur les rÃ©seaux de P2P et les sites Warez. Ces logiciels permettent de gÃ©nÃ©rer des clÃ©s afin de dÃ©verrouiller des logiciels payants.

La fourniture gratuite de ces gÃ©nÃ©rateurs de clÃ© doit vous alerter sur son rÃ©el but. En Â« offrant Â» ces logiciels, les pirates fournissent aussi un bouquet de malwares capable dâ□□infecter lâ□□ordinateur de la victime et dâ□□en prendre le contrÃ´le.