

G-Data : Le top 10 des menaces du mois de mai 2010

S curit 

Post  par : JPilo

Publi e le : 7/6/2010 0:00:00

G Data Software AG,  diteur de solutions de s curit  pour les particuliers et les entreprises, publie son classement des dangers pour le mois de mai

JS:Pdfka-OE [Expl] qui exploite une faille PDF est encore en t te. Mais derri re, les chevaux de Troie montent en puissance en occupant trois des cinq premi res places.

Le top 5 comment  et les conseils pour se prot ger :



1 re place : JS:Pdfka-OE [Expl]

Avec 3,6 % des d tections, cet exploit PDF tient encore le haut du podium. Il tire avantage des vuln rabilit s JavaScript dans les programmes PDF. Il suffit d ouvrir un fichier PDF infect  pour que le cybercriminel acc de   l ordinateur de sa victime.

  N ouvrez pas les fichiers provenant de destinataires inconnus ou ceux issus de cha nes de diffusion.

2 me place : WMA:Wimad [Drp]

Cet injecteur de cheval de Troie gagne 2 places. Il se pr sente comme un fichier audio WMA l gitime et invite l utilisateur   installer un Codec vid o.   d fait de vid o l infection est bien pr sente.

  Lorsque vous souhaitez visionner une vid o (g n ralement d actualit ) sur un site que vous d couvrez pour la premi re fois (souvent en langue anglaise) n acceptez aucun t l chargement de codec.

3 me place : Worm.Autorun.VHG

Ce vers exploitant l'Auturun de Windows se diffuse à partir de clé USB ou de disques durs externes.

Avant de transférer sur votre ordinateur des données provenant de supports de stockage externe, faites un scan antivirus des données.

4^{ème} place : Trojan.PWS.Kates.Z

Ce cheval de Troie est spécialisé dans le vol de données confidentielles, principalement de mots de passe. Il interdit l'exécution des fichiers .bat ou .reg sur les systèmes infectés. Il se protège ainsi contre des mesures de nettoyage.

Rang	Nom	Pourcentage	Tendance*
1	JS:Pdfka-OE [Expl]	3.6	↔
2	WMA:Wimad [Drp]	3.2	↗
3	Worm.Autorun.VHG	2.1	↔
4	Trojan.PWS.Kates.Z	0.9	↑
5	Win32:MalOb-BD [Cryp]	0.8	Nouveau
6	Win32:Rodecap [Trj]	0.7	↓
7	HTML:Iframe-inf	0.7	↘
8	Java:Djewers-N [Trj]	0.6	Nouveau
9	Application.Keygen.BG	0.5	Nouveau
10	Saturday 14th-669	0.4	↓

* La tendance indique la différence de rang par rapport au mois précédent

↑ : + > 2 ↗ : + 1 or 2 ↔ : ± 0 ↘ : - 1 or 2 ↓ : - > 2

Protégez votre système avec un antivirus et réalisez des analyses antivirus régulières de vos disques durs.

5^{ème} place : Win32:MalOb-BD [Cryp]

Ce cheval de Troie fait son entrée dans le top 10 et se positionne directement à la cinquième place. Il abaisse les paramètres de sécurité des systèmes infectés et télécharge ensuite de nouveaux malware à partir de serveurs distants. Il est souvent lié à de faux antivirus, des bots, du ransomware ou toute autre activité nuisible.

Utilisez un pare-feu. En cas d'alerte de celui-ci vérifiez bien que le programme qui souhaite communiquer via Internet est légitime. En cas de doute, utilisez les modules d'information du pare-feu ou, à défaut, recherchez le nom du programme douteux dans un moteur de recherche Internet.