Comunicat de presa G Data 2010

Clasamentul malware al lunii mai 2010 ne arata calcaiul lui Ahile al Internet-ului

Cyber-Infractorii exploateaza neglijenta si curiozitatea utilizatorilor

Bucuresti (Romania), 11 iunie 2010 – Actualul specialist in securitate al G Data publica topul celor 10 amenintari din luna mai. JS: Pdfka-OE [Expl], un malware care exploateaza vulnerabilitatea fisierelor PDF, este din nou in fruntea clasamentului in aceasta luna. De remarcat: trei dintre malware-urile din topul 5 al acestei luni se dovedesc a fi Troieni.

Eddy Willems, responsabilul cu securitatea al G Data declara :"In luna mai, am descoperit mai multi Troieni decat in luna aprilie. Am observat o crestere atat in numarul total al Troieni-lor, cat si in tipurile de Troieni in topul 10 al acestei luni."

Acest fapt nu il surprinde pe Willems: "Aceasta tactica este literalmente una invechita: eficienta ei fiind dovedita in Grecia antica." Nivelul de succes al acestora si al altor tipuri de malware este una din ingrijorarile lui Willems:" Faptul ca malware-ul inca prospera se datoreaza neglijentei utilizatorilor. De multe ori, ei nu isi securizeaza suficient PC-ul si de multe ori amana instalarea actualizarilor de software. In acelasi timp, multi dintre ei cad in capcana infractorilor, care isi imbunatatesc siretlicurile ingineriilor sociale. "In concluzie, Willems declara: "Neglijenta si curiozitatea pot transforma utilizatorul in calcaiul lui Ahile al Internetului."

Rank	Name	Percentage	Trend*
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	new
6	Win32:Rodecap [Trj]	0.7	⇘
7	HTML:Iframe-inf	0.7	⇩
8	Java:Djewers-N [Trj]	0.6	new
9	Application.Keygen.BG	0.5	new
10	Saturday 14th-669	0.4	⇗

* The trend indicates the difference in rank to the previous month

⇧ + > 2 ⇗ + 1or 2 ⇔ ± 0 ⇘ - 1 or 2 ⇩ - > 2

Percentage of Top10, May 2010:	13,4%
Total # of detections, May 2010:	936.420
Difference total # of detections April 2010 - May 2010:	+11,3%

Informatii despre 5 dintre cele mai importante amenintari ale lunii mai:

JS:Pdfka-OE[Expl]

Acesta este un *exploit* care incearca sa profite de vulnerabilitatile din motoarele JavaScript ale programului PDF. *Exploit-ul* se declanseaza atunci cand utilizatorul deschide un document PDF. Daca patrunderea in computerul victimei se face cu succes, se introduce o cantitate considerabila de continut malware.

WMA:Wimad[Drp]

Acest Troian pretinde a fi un audiofile legitim in format .wma sau alt format multimedia cum ar fi .mp3 sau .wmy. Daca este ascultat cu Windows Media Player deschide un website si cere un download al unui codec. O executare a fisierului activeaza mai multe atacuri malware asupra PC-ului. Fisierele infectate sunt deseori raspandite prin intermediul retelelor p2p.

Worm.Autorun.VHG

Un *worm* care se raspandeste cu ajutorul functiei autorun.inf in sistemele de operare Windows. Se foloseste de dispozitivele de stocare detasabile cum ar fi stick USB si HDD-uri portabile. Este un *worm* pentru Internet si retea care exploateaza vulnerabilitatea CVE-2008-4250 a Windows.

Troian.PWS.Kates.Z

Acesta este un Troian, care este specializat in furtul de informatii confidentiale si a parolelor esentiale. O infectare cu acest Troian din famillia Trojan.PWS.Kates rezulta in transformarea fisierelor .bat si .reg in ne-executabile. Windows Explorer se inchide de indata ce utilizatorul incearca sa lanseze regedit.exe, cmd.exe sau TotalCommander.

Win32:MalOb-BD [Cryp]

Acest Troian micsoreaza setarile de securitate ale sistemelor infectate si downloadeaza mai multe coduri malware. Este corelat cu software-uri antivirus false, bot-uri, *ransomware* si multe alte activitati oneroase.

-###-