Comunicat de presa G Data 2010

Atacurile PDF-cea mai mare amenintare a PC-urilor

Cel mai bine clasat new entry in Top 10 Malware al lunii aprilie compromite conturile private

Bucuresti (Romania), 18 mai 2010 – Raspandirea codurilor malware a luat proportii din nou in luna aprilie. De aceasta data, infractorii par sa se axeze in special pe bresele de securitate din programele de citire a formatului PDF. Acestea sunt principalele doua concluzii din raportul lunar despre malware al G Data. In aprilie, exploit-ul JS:Pdfka-OE este fara indoiala numarul unu in Top 10 Malware. Cel mai bine clasat new entry al lunii este Win32:Rodecap (Trojan), care este proiectat pentru a compromite serviciile de e-mail online, cum ar fi Yahoo, Hotmail si Google Mail.

"Exploatarea breselor de securitate in programele de computer este o modalitate de a infecta cu succes computerele cu malware. Cu cat este mai mare circulatia unei aplicatii, cu atat mai mult atrage interesul dezvoltatorilor de malware care vor sa ii exploateze vulnerabilitatile", explica Ralf Benzmuller, managerul Laboratoarelor G Data. "Un alt pericol subestimat este Worm.Autorun.VHG, care foloseste functia Autorun pentru a se raspandi prin stick-uri USB sau hard disk-uri externe. Persoanele carora nu le este necesara in mod special functia Autorun, ar trebui sa o dezactiveze, pentru mai multa siguranta."

Malware in April 2010

	Name	Percentage	Trend*
1	JS:Pdfka-OE [Expl]	11,4 %	↔
2	Win32:Rodecap [Trj]	1,7 %	new
3	Worm.Autorun.VHG	1,7 %	↘
4	WMA:Wimad [Drp]	1,3 %	↘
5	Saturday 14th-669	1,2 %	↘
6	HTML:Iframe-inf	1,0 %	↘
7	Trojan.PWS.Kates.Z	1,0 %	new
8	Trojan.Boaxxe.X	0,8 %	new
9	Win32.Sality.OG	0,6 %	↑
10	Win32:Crypt-GBX [Trj]	0,6 %	new

* The trend shows change in position in comparison to the previous month.

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

* Tendinta arata o schimbare de pozitie in comparatie cu luna precedenta.

Documentele PDF sunt considerate de regula inofensive, majoritatea computerelor avand instalate programe de citire a documentelor PDF. Totusi, functia JavaScript transforma un PDF intr-un format posibil periculos: un Acrobat JavaScript, care este incorporat intr-un PDF, este infectat si utilizat pentru a pregati atacuri, sau contine el insusi brese, care sunt mai apoi folosite de catre atacatori pentru a strecura propriile lor coduri malware. De aceea, atunci cand este posibil, compatibilitatea JavaScript a cititorului ar trebui sa fie inchisa. O alta masura de siguranta importanta este de a mentine cititorul actualizat, pentru a fi pregatit si protejat impotriva noilor atacuri malware.

Metodologie
Initiativa de Informare despre Malware (The Malware Information Initiative) se axeaza pe sprijinul comunitatii online, fiecare client al unei solutii de securitate G Data putand participa la aceasta initiativa. Singura cerinta este ca functia sa fie activata in cadrul programului G Data. Astfel, raportul dupa un atac malware contracarat cu succes este trimis, in mod anonim, catre Laboratoarele G Data Security, unde informatia este apoi colectata si evaluata statistic.

-###-