G Data press release 2015

G DATA: Programe malware infiltrate construiesc botneti

E-mail-uri ce contin abonamente feroviare false incearca sa atraga utilizatorii in capcana.

Bucuresti (Romania) 20.03.2015

Expertii furnizorului de securitate german G DATA au descoperit o serie de programe malware care au ca scop construirea unui botnet ce poate fi controlat folosind aceeasi server de comanda si control. Cele doua cazuri de malware pe care analistii le-au investigat folosesc rute semnificativ diferite de infectie. Expertii cred ca acest atac a fost planificat de catre unul sau mai multi autori, distribuind malware in masa, astfel incat botnetii sa poata fi apoi vanduti sau inchiriati. Malware-ul se autodistribuie prin comenzile macros din documente Word manipulate, trimise atasate in e-mail-uri. In anumite cazuri, infractorii trimit o factura falsa a unor abonamente pentru mijloace de transport pe cale ferata. Solutiile de securitate G Data detecteaza malware-ul si previne infectia.

“Malware-ul se comporta ca o papusa Matryoshka, dezvaluind treptat adevaratul sau potential", explica Ralf Benzmuller, seful G DATA SecurityLabs. "Noi banuim ca sistemele infectate sunt destinate utilizarii in calitate de computere zombie infectate cu botnetul Andromeda / Gamarue".

E-mail-uri cu abonamente pe calea ferata pretinse a reprezenta o factura

Prin deghizarea malwareului intr-o factura a unui abonament de tren, infractorii incearca sa deruteze utilizatorii. Beneficiarii sunt indemnati sa deschida documentul Word atasat si sa activeze comenzile macro. Odata ajuns pe calculator, malware-ul incearca sa-si mascheze actiunile cu scopul de a construi un botnet. Infractorii cibernetici pot controla apoi sistemele infectate de la distanta, fara ca proprietarii sa fie constienti de asta.

Ce este macro?

Comenzile macro sunt folosite pentru a automatiza sarcinile, astfel incat acestea pot fi executate cu un singur click. Acestea sunt de obicei dezactivate in pachetele Office, deoarece acestea pot reprezenta un risc de securitate. Dupa cum demonstreaza acest exemplu, infractorii cibernetici pot exploata aceasta functie utila pentru scopurile lor rau intentionate si determina utilizatorii sa activeze comenzile. Acest lucru permite malware-ului sa se furiseze si sa infecteze sistemul.

Informatii detaliate pot fi gasite pe G DATA SecurityBlog:

https://blog.gdatasoftware.com/blog/article/the-andromedagamarue-botnet-is-on-the-rise-again.html