G DATA press release 2017

Vault 7: Armele cibernetice ale CIA

Expertii G DATA Security, Eddy Willems si Ralf Benzmuller, au analizat dezvaluirile Wikileaks.

Bucuresti (Romania) 13.03.2017

Documentele confidentiale divulgate despre CIA dezvaluie activitatile de hacking, atat pe componente hardware, cat si pe componente software ale agentiei intre 2013 si 2016. Acestea mentioneaza explicit tinte precum dispozitive iPhone, Android, Linux, Windows sau Smart TV. Producatorii de securitate sunt si ei inclusi in lista. Pare ca nicio componenta a unui sistem hardware, software sau sistem de operare nu este in siguranta in fata armelor cibernetice ale CIA. Expertii G DATA, Eddy Willems si Ralf Benzmuller, au analizat documentele disponibile si si-au expus punctele de vedere intr-un articol pe blog.

Capabilitati extinse

Gratie celebrelor dezvaluiri facute de Snowden in urma cu cativa ani, astazi, nu prezinta nicio surpriza informatia ca agentiile de informatii ar fi angajate in activitati de spionaj. Ceea ce surprinde, insa, este amploarea si extinderea activitatilor. Acest lucru este valabil si in cazul documentelor Vault7. Acestea nu fac referire doar la colectarea de vulnerabilitati din computere sau servere. Conform documentelor, agentia vizeaza toate dispozitivele conectate la Internet. Dispozitive cu Android si iOS, routere si televizoare inteligente, sunt la fel de viabile ca tinte ca si dispozitivele incorporate si produsele hardware IoT. Instrumentele CIA includ chiar si capabilitati de hacking pentru echipamente industriale SCADA sau sisteme utilizate in industria auto. In acelasi timp, sunt luate masuri ample pentru ascunderea acestor aceste instrumente si sunt folosite tehnici care ascund sustragerile de date. “S-ar parea ca fiecare componenta dintr-o tehnologie cu o oarecare relevanta in piata, este atent evaluata pentru a putea fi utilizata in spionaj si razboi cibernetic”, spune Eddy Willems, G DATA Security Evangelist.

Suspiciunile vechi sunt confirmate

Ralf Benzmuller, Executive speaker la G DATASecurity Labs, clarifica faptul ca "Ar fi naiv sa credem ca dezvoltarea armelor cibernetice este controlata doar de catre SUA. Noi credem ca si alti membrii ai comunitatilor de informatii au dezvoltat programe similare de ani de zile, cu fonduri in valoare de milioane de euro". "Cele mai recente scurgeri nu au facut decat sa confirme ceea ce multi experti in securitate IT au suspectat de foarte mult timp. Avand echivalentul cibernetic al unui Broken Arrow, in cazul in care infractorii ar pune mana pe astfel de arme cibernetice, ar fi extrem de problematic, ca sa nu spunem mai mult. Consecintele ar putea fi catastrofale."

Cu toate acestea, expertii in securitate de la G DATA nu cred ca instrumentele de spionaj au fost sau sunt utilizate in prezent pe scara larga impotriva utilizatorilor de Internet obisnuiti. Natura instrumentelor sugereaza ca acestea sunt mai degraba destinate utilizarii in atacuri directionate. Multi producatori au inceput deja sa lucreze pentru a repara defectele de securitate dezvaluite in documentele CIA.

Pacalirea solutiilor de securitate

Numerosi furnizori de securitate, inclusiv G DATA, au fost mentionati in documentele CIA. Se pare ca CIA a dezvoltat instrumente care sunt concepute a ocoli orice solutie de securitate, care este implementata la punctul tinta. Totusi, exista putine informatii despre aceast subiect in documentele oferite publicitatii (de exemplu, apar liste incomplete ale proceselor) si care fac referire doar la cativa furnizori. La acest moment, nu sunt alte detalii publice oferite, in afara celor oferite despre acesti cativa vendori, sectiunile corespunzatoare fiind clasificate de WikiLeaks drept "secrete". G DATA a contactat WikiLeaks pentru a obtine informatiile care fac referire la solutiile proprii.

Comentariul integral ce face referire la documentele WikiLeaks este disponibil pe blog-ul G Data Security: https://blog.gdatasoftware.com/2017/03/29561-wikileaks-vault7