



G DATA press release 2017

## **WannaCry: Ransomware-ul care ataca utilizatorii privati si companiile din intreaga lume**

**Expertii in domeniul securitatii datelor de la G DATA publica analize actualizate in mod constant si ofera recomandari celor afectati cu privire la ce trebuie sa faca.**

Bucuresti (Romania) 16.05.2017

Programul ransomware WannaCry a lovit companii din intreaga lume - au fost afectate chiar si infrastructuri critice precum spitale sau furnizori de energie. Deutsche Bahn a fost, de asemenea, una dintre victimele importante ale atacurilor cibernetice. Mecanismul de infectare din WannaCry implica un exploit care a fost descoperit de serviciul secret al SUA, NSA. Troianul de extorcare ajunge pe calculatoare printr-o bresa de securitate din sistemul de operare Windows. Microsoft a inchis, de fapt, vulnerabilitatea cu o actualizare in martie 2017. Managerii IT si persoanele fizice trebuie sa reactioneze imediat si sa instaleze actualizarile de securitate cat mai urgent posibil. Utilizatorii G DATA sunt protejati impotriva WannaCry.

"Valul de infectii care a izbucnit vineri a lovit utilizatori casnici, companii, institutii publice si furnizori de utilitati ", explica Tim Berghoff, G DATA Security Evangelist. "Cand a fost publicat documentul WikiLeaks, ne-am exprimat ingrijorarea ca aceste informatii vor fi folosite de infractorii cibernetici pentru atacuri, in cazul in care vor avea acces la el. Succesul lui WannaCry a eclipsat deja efectele produse de programele ransomware Locky si CryptoLocker."

### **Infractorii folosesc instrumentele NSA**

Incidentul confirma unele temeri care au aparut ca urmare a dezvaluirilor WikiLeaks. E evident ca infractorii au reusit sa foloseasca un instrument din arsenalul serviciului secret in scopuri infractionale. Un exploit numit "Eternalblue" face parte dintr-o colectie de fisiere din surse NSA care a fost facuta publica in aprilie de grupul de hackeri "Shadow Brokers". Cum si alte instrumente au facut parte din acea scurgere de informatii, scenariul se poate repeta, iar alte instrumente ale serviciului secret ar putea fi folosite de catre infractorii cibernetici pentru a initia alte atacuri.

### **Instalati urgent actualizarile de securitate**

Incidentele dramatice de zilele trecute arata ce consecinte pot aparea daca actualizarile nu sunt instalate in timp util. Bresa de securitate exploatarea in atac a fost inchisa de Microsoft in martie - chiar si asa, WannaCry a fost un succes pentru atacatori. Organizatiile guvernamentale, companiile si persoanele fizice ar trebui sa se gandeasca foarte repede la modul in care pot inchide bresele de securitate respective. Managerii IT din companii ar trebui



sa verifice utilizarea gestionarii patch-urilor pentru a permite actualizarea rapida pentru fiecare computer din retea.

Analiza atacurilor, actualizata in permanenta de expertii G DATA Security poate fi gasita pe G DATA Security Blog <https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign>