Nr. 1308 din 25 octombrie 2018

**POLIȚIA ROMÂNĂ A LUCRAT, ALĂTURI DE EUROPOL ȘI BITDEFENDER, LA UN DECRIPTOR PENTRU CEL MAI RĂSPÂNDIT RANSOMWARE DIN LUME**

***Poliția Română, cu sprijinul Europol, Bitdefender și al altor instituții de aplicare a legii, a lucrat la dezvoltarea unui utilitar gratuit pentru recuperarea datelor blocate, destinat victimelor celei mai recente versiuni a clasei de ransomware GandCrab.***

Autorităti de aplicare a legii din mai multe state (Bulgaria, Franța, Italia, Olanda, Polonia, UK – NCA și Metropolitan Police, Ungaria, USA – FBI) au făcut front comun, împreună cu Poliția Română și Europol pentru combaterea acestei amenințări, considerată a fi cea mai prolifică formă de ransomware a momentului.

Amenințarea GandCrab a făcut pagube de sute de milioane de dolari, unele inclusiv în România. Decriptorul le permite victimelor să primească acces la datele criptate fără să mai plătească recompensă atacatorilor și poate decripta versiunile 1, 4 și 5 ale GandCrab.

Lansarea acestui utilitar este o descoperire revoluționară care arată cât de eficientă este colaborarea dintre companiile de securitate cibernetică și instituțiile de aplicare a legii. Soluția de decriptare, la care s-a lucrat mai multe luni de zile, le redă victimelor accesul la viața digitală fără niciun cost.

Versiunea ransomware GandCrab a fost extrem de activă din luna ianuarie și a operat folosind un model de afiliere, prin care dezvoltatorii îl ofereau ca serviciu plătit celor interesați să îl răspândească, cerând în schimb un anumit procent din încasări. GandCrab se răspândește prin vectori de atac multipli, precum emailuri de tip spam și campanii de malware.

În 2018, GandCrab a suferit transformări radicale, mai ales după ce Poliția Română a pus, la începutul acestui an, la dispoziția publicului, un instrument de decriptare pentru prima versiune a acestuia, dezvoltat tot cu sprijinul companiilor private, instituțiilor locale și internaționale de aplicare a legii.

Pentru a preveni infectarea cu ransomware, utilizatorilor li se recomandă să păstreze copii ale datelor importante, să folosească o soluție de securitate performantă și să evite să acceseze linkuri sau fișiere din e-mail-uri nesolicitate.

Proiectul No More Ransom a fost lansat în iulie 2016 de poliția națională olandeză și Europol, instituția de combatere a criminalității la nivelul Uniunii Europene, cu scopul de a crește nivelul de colaborare dintre sectoarele public și privat în lupta contra ransomware. Pe nomoreransom.org, utilizatorii pot afla informații suplimentare despre ransomware și modul în care se pot feri de această amenințare.

Întreaga activitate de cooperare investigativă internațională s-a făcut prin intermediul proiectului EMPACT, prioritatea Cybercrime Attacks Against Information Systems. Ciclului de politici europene EMPACT au ca prioritate lupta împotriva criminalității organizate, în perioada 2018-2021.

Utilitarul de decriptare pentru GandCrab poate fi descărcat în mod gratuit aici: <http://download.bitdefender.com/am/malware_removal/BDGandCrabDecryptTool.exe>

De asemenea, toate utilitarele de decriptare pot fi găsite aici:

https://www.nomoreransom.org/en/index.html