



SIMPLY
SECURE

G DATA press release 2016

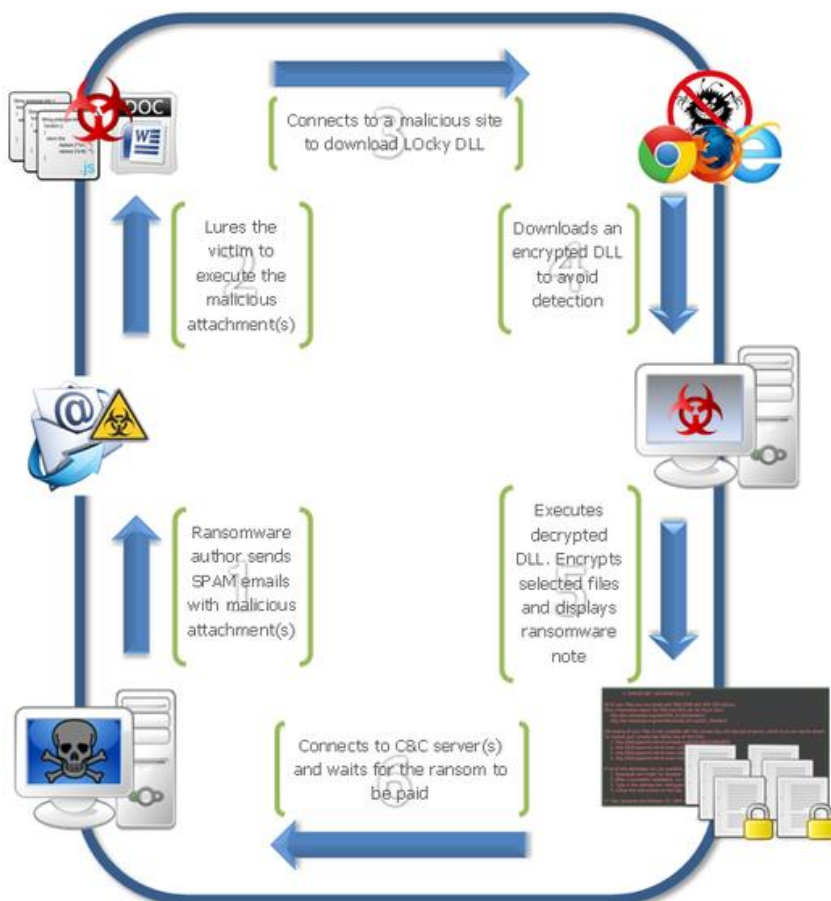
O noua versiune a programului ransomware Locky este din nou in circulatie

Expertii in securitate de la G DATA analizeaza troianul de extorcare.

Bucuresti (Romania) 24.10.2016

Troianul Locky a facut senzatie in randul utilizatorilor de computere si in mass-media acum aproximativ opt luni. O noua versiune a malware-ului este distribuita din nou, iar fisierele sunt criptate cu extensia .ODIN. Analistii de la G DATA au examinat programul ransomware cu atentie si au prezentat rezultatele pe blog-ul de securitate G DATA. Utilizatorii solutiilor de securitate G DATA sunt protejati: malware-ul investigat este cunoscut sub numele de Script.Trojan-Downloader.Locky.CQ sau Win32.Trojan-Ransom.Locky.CQ.

Analiza efectuata de catre expertii de securitate G DATA poate fi gasita pe blog-ul de securitate: <https://blog.gdatasoftware.com/2016/10/29245-meet-the-latest-member-of-the-locky-family-odin>





Cum va puteti proteja?

- Cea mai buna protectie impotriva programelor ransomware este de a efectua backup-uri regulate. Datele trebuie sa fie stocate intr-o mediu de stocare separat de sistem. Daca rulati o copie de rezerva pe un hard disk extern, decuplati-l dupa ce backup-ul s-a finalizat si asigurati-va ca acesta este offline atunci cand nu este necesar sa fie online. Cu ajutorul unui backup regulat va puteti asigura ca nu pierdeti niciun fel de date in cazul unei infectii reale cu ransomware si puteti restaura cu usurinta sistemul. Atunci cand faceti acest lucru, asigurati-va ca utilizati un mediu de stocare securizat.
- O infectie poate fi prevenita in cazul in care utilizatorul nu se autentifica intotdeauna cu contul sau de administrator, ci stabileste si se autentifica cu un cont de guest, in schimb. Cum un astfel de cont are drepturi limitate, ransomware-ul nu poate patrunde foarte adanc in sistem si, in mod ideal, nu va aduce prejudicii.
- In plus, trebuie sa efectuati actualizari periodice ale sistemului de operare. In acest fel, puteti inchide bresele de securitate. Acelasi lucru este valabil si pentru browser si orice program instalat pe sistem.
- Protectia browser-ului este utila pentru a va proteja de script-uri periculoase si pentru a preveni descarcarea accidentala a malware-ului.
- E-mailurile false si frauduloase pot fi anihilate prin intermediul unui software special de securitate. Astfel de e-mailuri nu mai sunt o problema, software-ul antivirus detecteaza si sterge programele malware.

-###-