Locky letámadta Európát

**



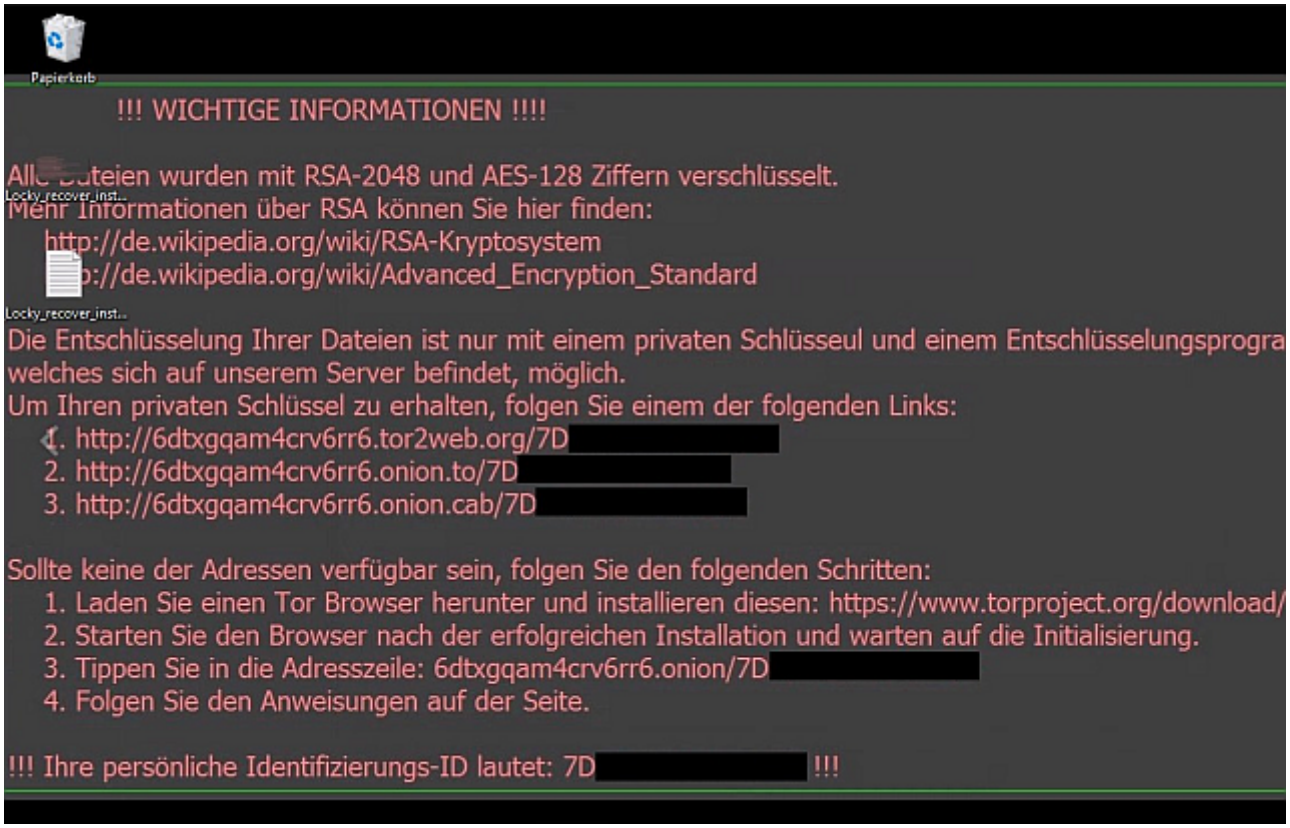
Locky** egy trójai program, egészen pontosan egy **ransomware**, ami brutális tempóban terjed immár Európában is, csak Németországban nagyjából **5000 új fertőzés**t regisztrálnak jelenleg az erre szakosodott cégek **óránként**.

> A ransomware olyan malware, azaz rosszindulatú számítógépes program, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek a hatására visszaállítja az eredeti állapotot. Forrás: Wikipedia

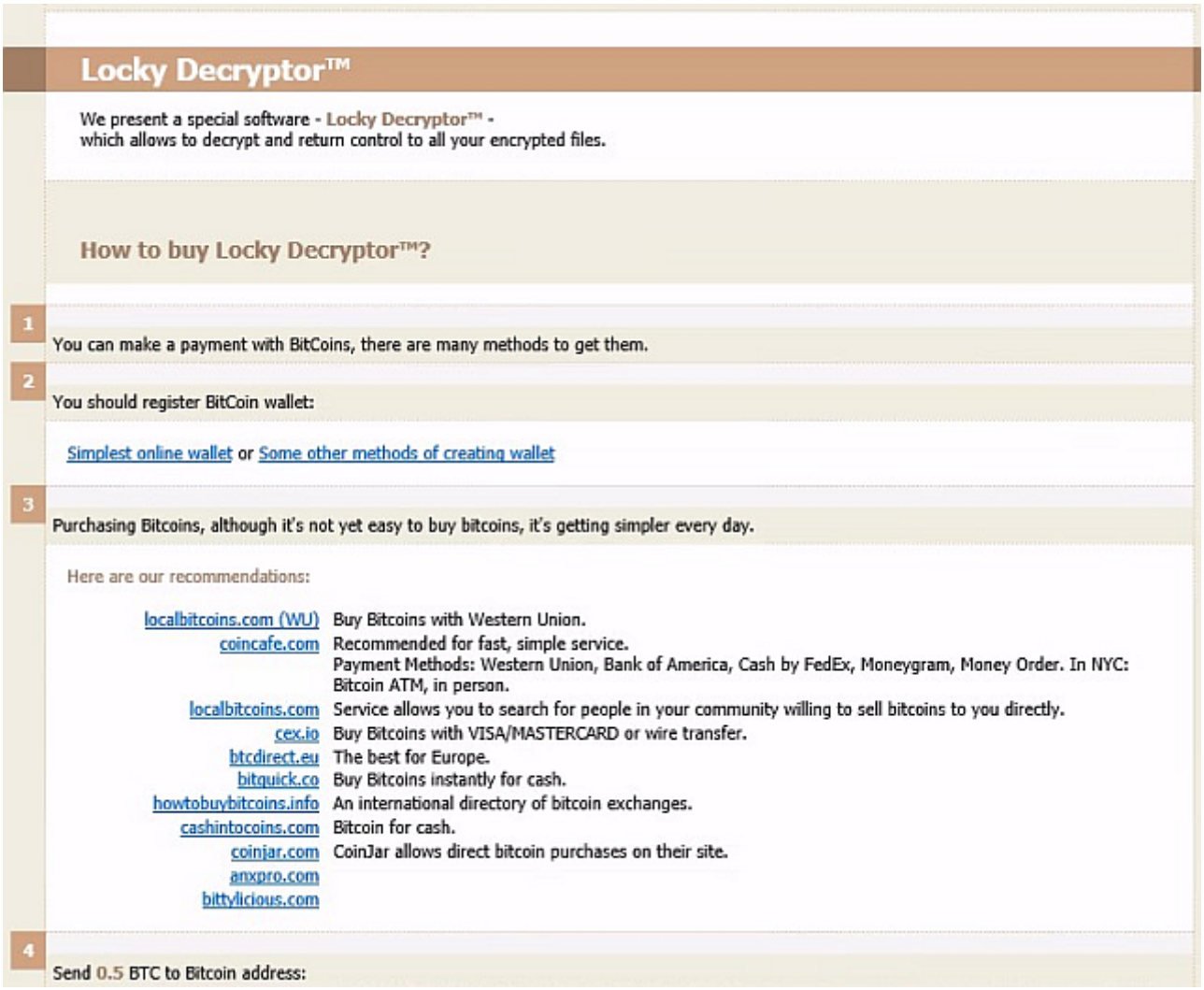
A kártevő jellemzően Excel vagy Word dokumentumok lévén terjed. A felhasználónak egy email érkezik, melyhez egy számla is érkezik a csatolmányban Word vagy Excel formában.

A tartalom megnyitás után **nem olvasható**, egy üzenet jelenik meg, mely szerint egy **makró aktiválásával** a betűsaláta majd láthatóvá válik; német változatban a következő szöveggel: *„Bitte Makros aktivieren, wenn die Datencodierung falsch ist”*. Lehet, hogy a szöveg is láthatóvá válik a makró lefutása után, de mellesleg egy trójai is felkerül ezzel a gépünkre *ladybi.exe* néven.

Ez azonnal futtatni kezd egy kódoló rutint, ami az általa fontosabbnak minősített fájlokat lekódolja. Teszi ezt ráadásul nem csak a saját gépünkön, hanem minden, a hálózaton elérhető tárhelyen is. Ráadásul – a **CERT** közlése szerint – olyan szervereket is megtalál a hálózaton, amik az adott gépről **nem is voltak map-olva**, illetve **a felhőben tárolt** adatokat is el tudja érni.



Szakértők szerint ez a trójai nem egy kispályás fejlesztés; valószínűleg több százezer gépet talált már meg a világon, ráadásul több nyelven, többfajta levél mellékleteként terjed. A kikódoláshoz az áldozatoknak természetesen fizetniük kell; egy elvileg vissza nem követhető Tor oldalon kell leperkálni a zsarolási díjat, természetesen bitcoin-ban.



Ezért a pénzért – a fenti ábrán fél bitcoin-ért (54 ezer forintért) egy programot, a *„Locky Decryptor”*-t kapjuk meg, ami alkalmas a fájlok kikódolására, de természetesen csak a mi gépünkön (más gépeken eltérő kulccsal kódolta le a kártevő a fájlokat).

A történetben **az egyetlen jó hír**, hogy ezt követően **a trójai valóban kikódolja** a túszul ejtett fájlokat. Nem biztos, hogy a Locky volt a tettes a Hollywood Presbyterian Medical Center esetén, hiszen a zsarolóprogramok meglehetősen nagy számban szedik áldozataikat a neten, mindenesetre nekik a hálózatuk kikódolása 40 bitcoinba fájt – a bitcoin pillanatnyi kurzusa szerint 1 bitcoin nagyjából 380 eurót kóstál, így a kikódolás végösszege a kórháznak nagyjából **4 és fél millió forintba** került nekik.

Érdemes megjegyezni, hogy van olyan ransomware is, ami a kódolás mellett a torrenttel letöltött fájlok listája alapján **jogvédőkkel vagy rendőrséggel fenyegetőzik**, és ez alapján követel pénzt, ahogy ez a lenti képen is látható (ez a kártevő nem azonos a bejegyzésben taglalt Locky-val):



Hogyan lehet védekezni a kártevők ellen

Ha már lekódolta a gépünket, sehogy. Ha van mentésünk a lekódolt fájlokról, akkor a kártevő és a kódolt állományok törlése után ezek visszaállíthatók. Ha nem, akkor sajna lehet a Decryptor útmutatása alapján spórolt pénzünket bitcoinra váltani.

Megelőzésként:

- Az Excelben és Wordben mindenképpen tiltani kell az automatikus makro-végrehajtást.
- Ismeretlen helyről érkező emaileket, főleg ha csatolmánnyal érkeznek, azonnal törölni kell.
- Egyrészt a fontos fájlokat mindig menteni kell, másrészt olyan helyre kell ezeket elpakolni, ami a mentést követően fizikailag leválasztható a gépünkről: USB-re, CD-re, DVD-re, külső merevlemezre, leporellóra.
- A mentést követően ezeket le is kell választani a gépünkről (a vírus minden, a hálózaton elérhető tartalmat kódolhat.)

Ez egy elfeledett sarka a netnek, örülök, hogy sikerült elvetődnöd ide!

Továbbra is keresek megjelenési lehetőséget az írásaim számára. Ha esetleg van ötleted, oszd meg velem! Elérhetőségeim az Impresszumban találhatók.

A passport.blog jelenlegi egyetlen megjelenési lehetősége a Facebook. Ha értesülni szeretnél az új bejegyzésekről, kövesd a Bolyongó Facebook oldalt.

Ha szeretnéd a bejegyzést kinyomtatni, vagy önálló formában menteni, ennek a legegyszerűbb módja a PDF formába konvertálás. Ezt a jobb oldali, fentről negyedik (Adobe) ikonnal teheted meg.

Eddigi bejegyzések a bolyongó.hu-n

Az összes bejegyzés ABC-be rendezett indexe itt található. A blog helyekhez köthető bejegyzései a google.maps térképen is megtalálhatók: A világ valódi csodái. A mostanában a blogon megjelent írások a főoldalon jelennek meg.

2026/05/28 18:05

Források

golem.de: Mehr als 5.000 Infektionen pro Stunde in Deutschland
heise.de: Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde
arstechnica.com: Hospital pays $17k for ransomware crypto key

2016, locky, vírus, ransomware, Európa, Németország, Excel, Word, macro, bitcoin, támadás, tech, lock, lekódol

Bejegyzésmegtekintések száma: 96

From:
https://mail.bolyongo.hu/ - **bolyongó**

Permanent link:
https://mail.bolyongo.hu/doku.php?id=passport:locky_letamadta_europat

Last update: **2026/08/22 08:32**