

# Locky letámadta Európát

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

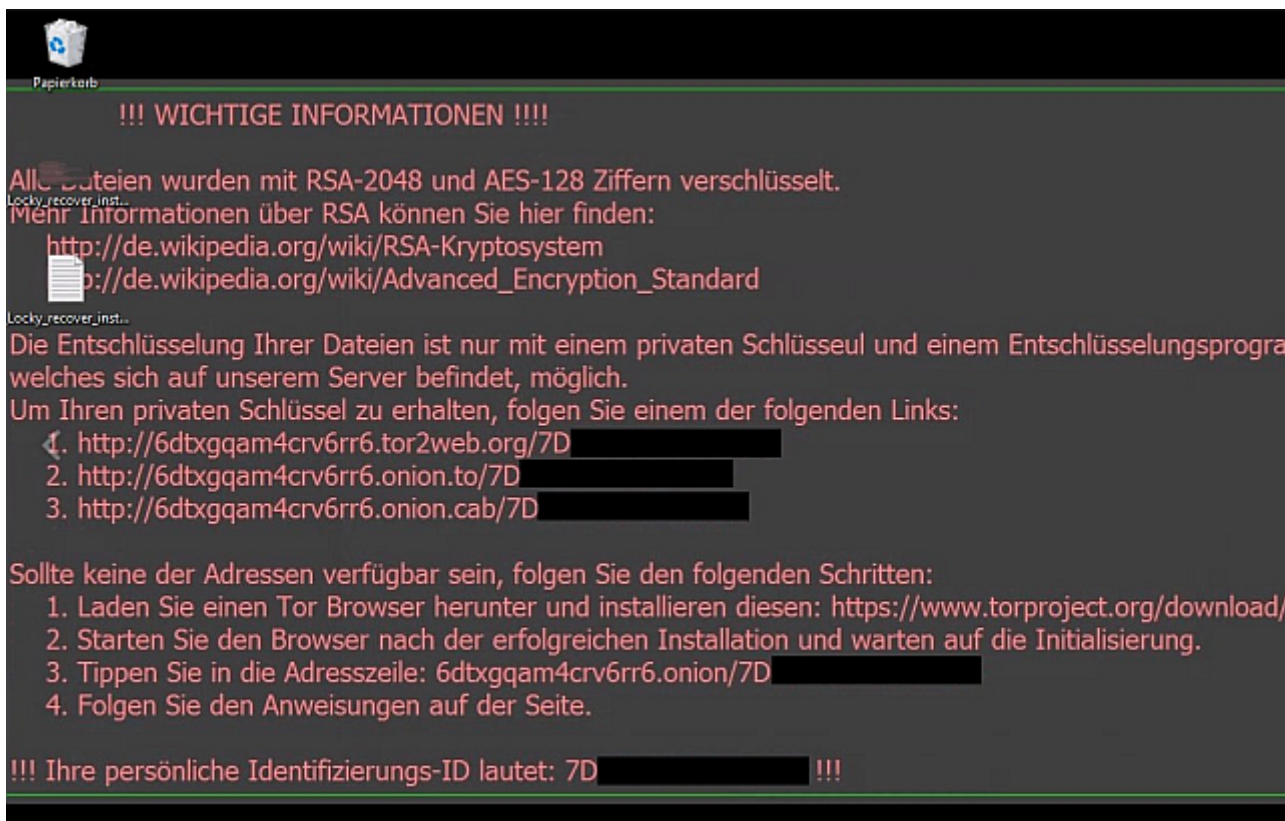


A ransomware olyan malware, azaz rosszindulatú számítógépes program, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból. Ez rendszerint azt jelenti, hogy használhatatlanná teszi a számítógépet vagy elérhetetlenné a rajta lévő adatokat, és csak pénzért vásárolható meg az a kód, aminek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

**Locky Decryptor™**

We present a special software - Locky Decryptor™ - which allows to decrypt and return control to all your encrypted files.

**How to buy Locky Decryptor™?**

- 1 You can make a payment with BitCoins, there are many methods to get them.
- 2 You should register BitCoin wallet:  
[Simplest online wallet](#) or [Some other methods of creating wallet](#)
- 3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.  
Here are our recommendations:  
  - [localbitcoins.com \(WU\)](#) Buy Bitcoins with Western Union.
  - [coincafe.com](#) Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
  - [localbitcoins.com](#) Service allows you to search for people in your community willing to sell bitcoins to you directly.
  - [cex.io](#) Buy Bitcoins with VISA/MASTERCARD or wire transfer.
  - [btcdirect.eu](#) The best for Europe.
  - [bitquick.co](#) Buy Bitcoins instantly for cash.
  - [howtobuybitcoins.info](#) An international directory of bitcoin exchanges.
  - [cashintocoins.com](#) Bitcoin for cash.
  - [coinjar.com](#) CoinJar allows direct bitcoin purchases on their site.
  - [anxpro.com](#)
  - [bittylicious.com](#)
- 4 Send 0.5 BTC to Bitcoin address:

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 túsul 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):

The screenshot shows a computer screen with a warning message from the United Kingdom Police. The message is titled "ATTENTION! Your PC is blocked due to at least one of the reasons specified below." and states that the user has violated copyright law. It also provides details about the user's IP address, country (United Kingdom), city, ISP, operating system (Windows 7 64-bit), and user name (User). To the right of the warning is a payment interface for Ukash and PaysafeCard, including a voucher number field and buttons for "Pay Ukash" and "Pay PaySafeCard".

## 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.

### Megelőzősként:

- Az Excelben és Wordben mindenképpen tiltani kell az automatikus makro-végrehajtást.
- Ismeretlen helyről érkező emaileket, főleg ha csatolmányal 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.)

**Kedves olvasóm!** Ha már idáig eljutottál az olvasásban, talán joggal feltételezhetem, hogy nem volt teljesen érdektelen számodra ez a bejegyzés. Jaj, le ne ixelj még; nem pénzt akarok tarhálni.

Pusztán annyit kérek, hogy ha van olyan ismerősöd, akivel jót tudnál vitatkozni az itt leírtakról, vagy csak simán megosztanád vele, kérlek, ne késlekedj!

Továbbra is keresek megjelenési lehetőséget az írásaim számára. Ha esetleg van ötleted, osszd meg velem! Elérhetőségeim az [Impresszum](#)ban található.

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](#).

2025/07/20 08:26

## 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: 114

From:

<http://bolyongo.hu/> - **bolyongó**

Permanent link:

[http://bolyongo.hu/doku.php?id=passport:locky\\_letamadta\\_europat](http://bolyongo.hu/doku.php?id=passport:locky_letamadta_europat)

Last update: **2021/04/13 19:47**

