CryptoLocker

Lance James

Head of Cyber Intelligence, Deloitte & Touche LLP

About the presenter

Lance James

Head of Cyber Intelligence, Deloitte & Touche LLP

- Author of "Phishing Exposed" and co-author of "Emerging Threat Analysis”
- Advisory board member of the Digital PhishNet
- Centre for Strategic Cyberspace + Security Science (CSCSS.org), creator of InvisibleNet (IIP/I2P)
- Co-Founder of Secure Science Corporation

Lance has more than a decade of experience in programming, network security, digital forensics, malware research, cryptography design & cryptanalysis, attacking protocols, and deep experience in information security, and has provided consultation to small start-ups, national and international governments, and Fortune 500 companies, including top American financial institutions.

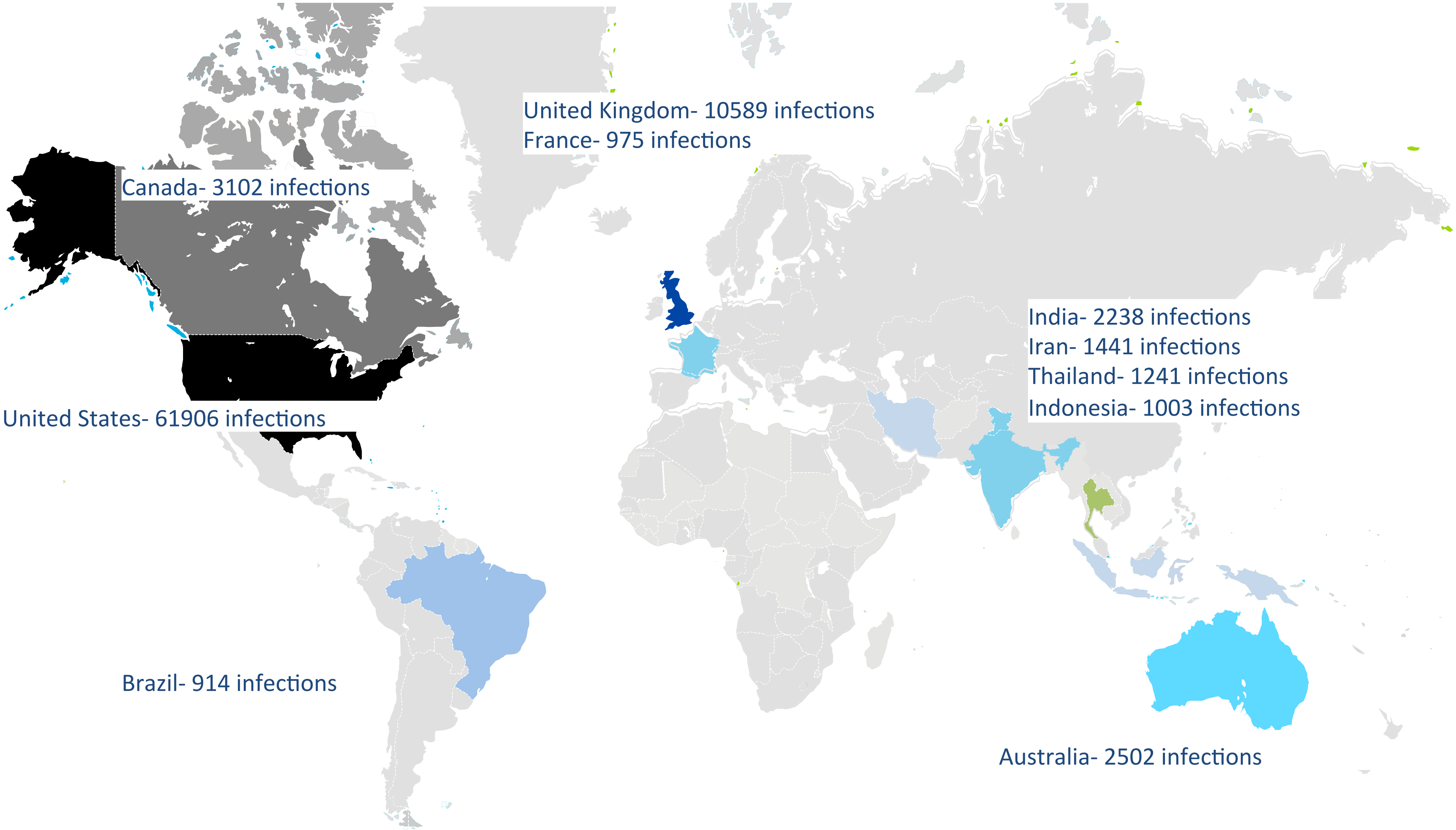
CryptoLocker

- RansomWare done right
  - RSA:2048 (decrypt key on server)
  - AES: 256
  - WinCrypt Library
- Generated domains
  - Act as proxies
  - Identified server in South Africa
  - Acquired domain generation algorithm (DGA) for prevention

Working Group

- Sinkhole establishment
  - Georgia Tech, and others
- Law enforcement
  - USA and abroad
- C1, C2, and C3 acquisition
  - Multi-tier network
- DGA reversing
  - Ahead of the threat

Snapshot CryptoLocker Infection



United Kingdom- 10589 infections
France- 975 infections

Canada- 3102 infections

United States- 61906 infections

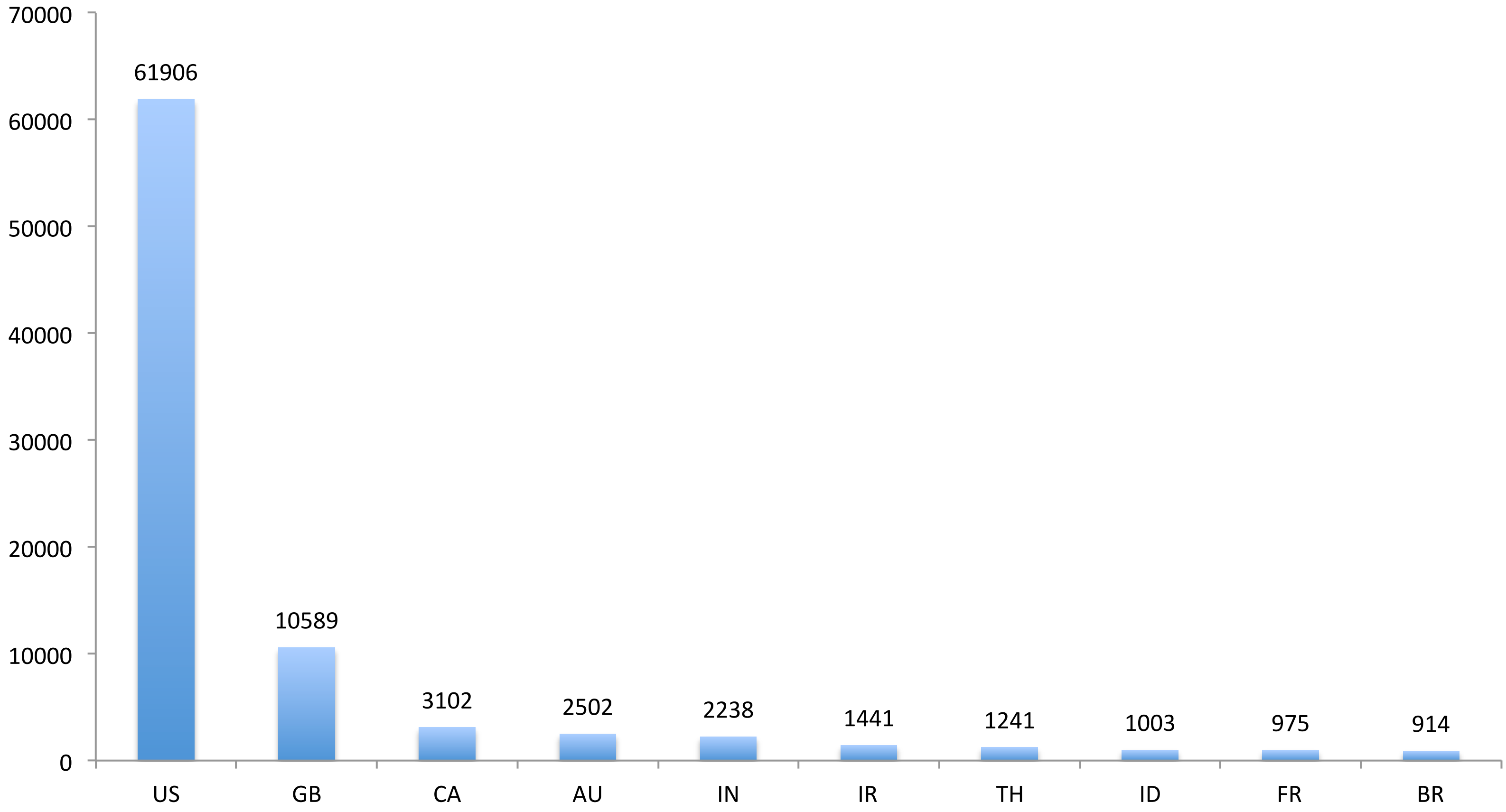
India- 2238 infections
Iran- 1441 infections
Thailand- 1241 infections
Indonesia- 1003 infections

Brazil- 914 infections

Australia- 2502 infections

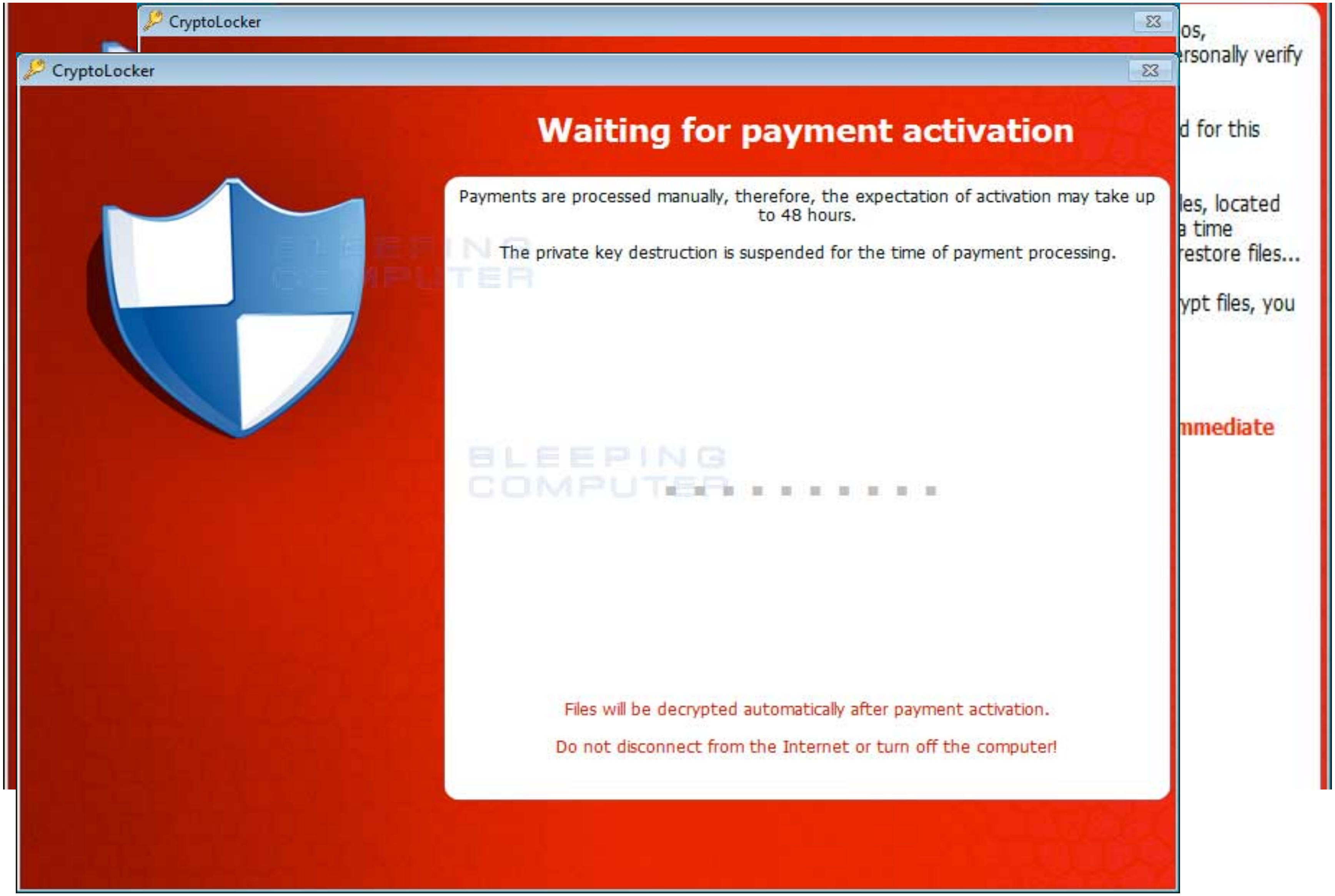
Source:* CryptoLocker Working Group - "Roy Arends, Nominet UK" Sinkhole data collected *Date: October 15 2013 – January 27 2014

Top 10 Cryptolocker Infections by Country



Source: **CryptoLocker Working Group - "Roy Arends, Nominet UK" Sinkhole data collected *Date: October 15 2013 – January 27 2014***

CryptoLocker



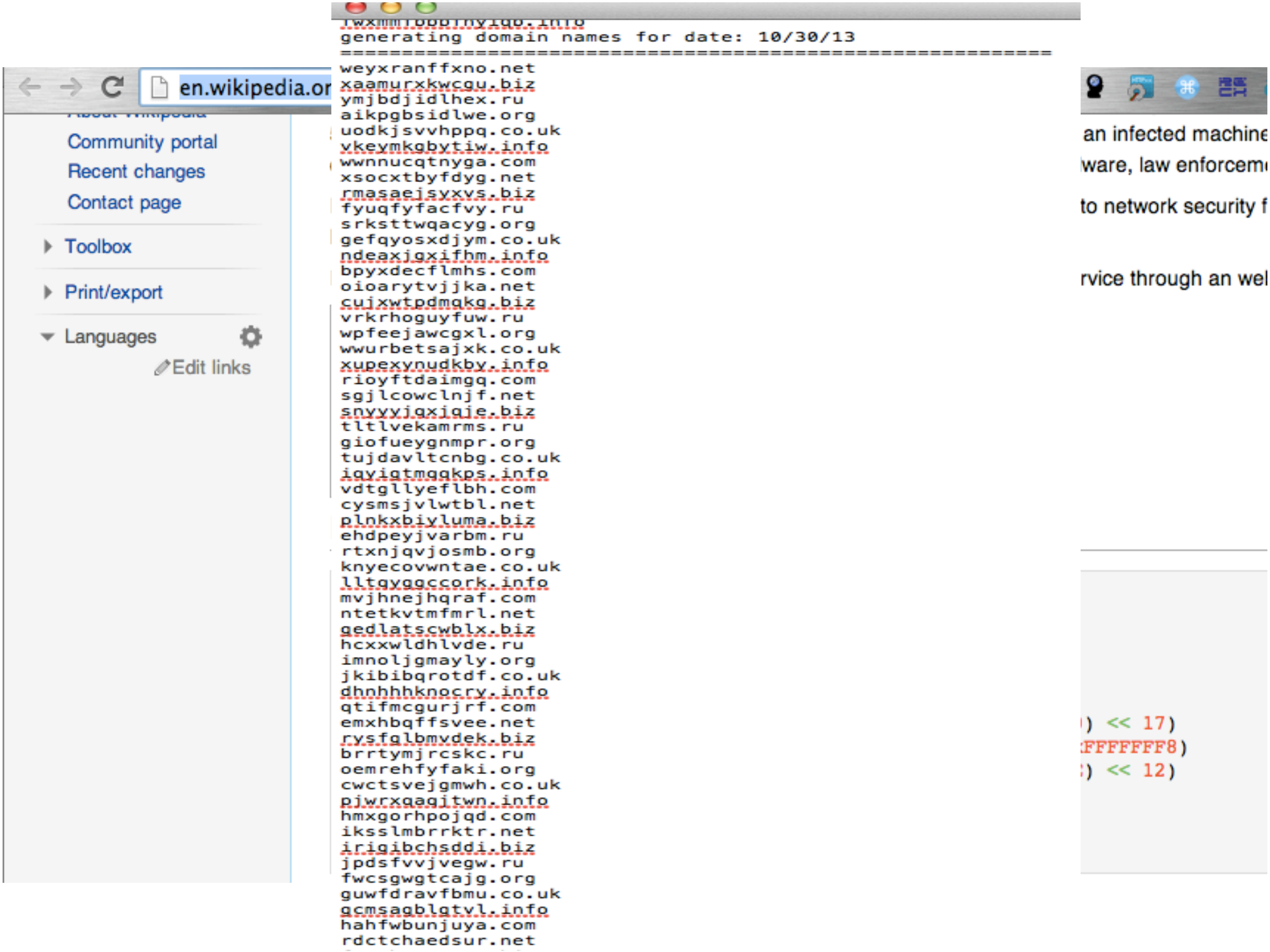
Waiting for payment activation

Payments are processed manually, therefore, the expectation of activation may take up to 48 hours.

The private key destruction is suspended for the time of payment processing.

Files will be decrypted automatically after payment activation.

Do not disconnect from the Internet or turn off the computer!



```
generating domain names for date: 10/30/13
==========================================================================
weyxranffxno.net
xaamurxkwcgu.biz
ymjbdjidlhex.ru
aikpgbsidlwe.org
uodkjsvvhppq.co.uk
vkeymkgbytiw.info
wwnnucqtnyga.com
xsocxtbyfdyg.net
rmasaejsyxvs.biz
fyuqfyfacfvy.ru
srksttwqacyg.org
gefqyosxdjym.co.uk
ndeaxjgxifhm.info
bpyxdecflmhs.com
oioarytvjjka.net
cujxwtpdmqkg.biz
vrkrhoguyfuw.ru
wpfeejawcgxl.org
wwurbetsajxk.co.uk
xupexynudkby.info
rioyftdaimgq.com
sgjlcowclnjf.net
snyyyjqxjqje.biz
tltlvekamrms.ru
giofueygnmpr.org
tujdavltcnbg.co.uk
iqyigtmqqkps.info
vdtgllyeflbh.com
cysmsjvlwtbl.net
plnkxbiyluma.biz
ehdpeyjvarbm.ru
rtxnjqvjosmb.org
knyecovwntae.co.uk
lltqyggccork.info
mvjhnejhqraf.com
ntetkvtmfmrl.net
gedlatscwblx.biz
hcxxwldhlvde.ru
imnoljgmayly.org
jkibibqrotdf.co.uk
dhnhhhknocry.info
qtifmcgurjrf.com
emxhbqffsvee.net
rysfglbmvdek.biz
brrtymjrcskc.ru
oemrehfyfaki.org
cwctsvejgmwh.co.uk
pjwrxqaqjtwn.info
hmxgorhpojqd.com
iksslmbrrktr.net
irigibchsddi.biz
jpdsfvvjvegw.ru
fwcsgwgtcajg.org
guwfdravfbmu.co.uk
gcmsagblgtvl.info
hahfwbunjuya.com
rdctchaedsur.net
```

Domain Generation Algorithm

- Characteristics
  - Random 4.0 bit/byte or higher
  - Generates 800-1020 domains per day
  - Only some will be used
    - There's a clue
  - Many use non-standard top level domains (TLDs)
    - .biz
    - .info
  - Static Pattern Analysis
    - Non-existent domains (NXD)
    - Why is my network making these requests?
    - Cluster NXD's
      - Entropy Scan/N-gram/Structure
      - TLD Scan