BITSIGHT

Botconf 2025 LT

The year is 2016, the name is SandiFlux (maybe)

João Godinho - TRACE

Double Fast Flux

- Domain with multiple A records and low TTL.
- Nameserver with multiple A records and low TTL.
- Low TTL for NS records.

```
;; ANSWER SECTION:
helpsscodds.in.         150     IN      A       95.86.30.3
helpsscodds.in.         150     IN      A       201.191.99.134
helpsscodds.in.         150     IN      A       119.204.11.2
helpsscodds.in.         150     IN      A       189.232.40.243
helpsscodds.in.         150     IN      A       109.175.17.10
helpsscodds.in.         150     IN      A       186.123.165.48
helpsscodds.in.         150     IN      A       58.151.148.90
helpsscodds.in.         150     IN      A       109.175.29.39
helpsscodds.in.         150     IN      A       154.144.253.197
helpsscodds.in.         150     IN      A       177.222.41.236
```

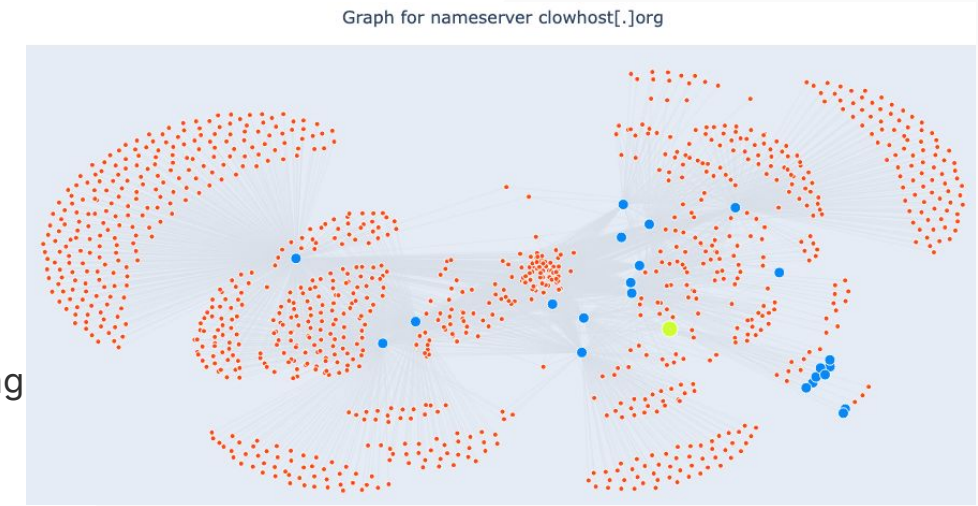
```
;; ANSWER SECTION:
helpsscodds.in.         150     IN      NS      ns2.dierjacrose.shop.
helpsscodds.in.         150     IN      NS      ns3.dierjacrose.shop.
helpsscodds.in.         150     IN      NS      ns4.dierjacrose.shop.
helpsscodds.in.         150     IN      NS      ns1.dierjacrose.shop.
```

```
;; ANSWER SECTION:
ns1.dierjacrose.shop.   150     IN      A       63.143.98.185
ns1.dierjacrose.shop.   150     IN      A       197.44.54.74
ns1.dierjacrose.shop.   150     IN      A       187.33.56.60
ns1.dierjacrose.shop.   150     IN      A       41.225.239.178
```

SmokeLoader domain registered on 2025-05-16

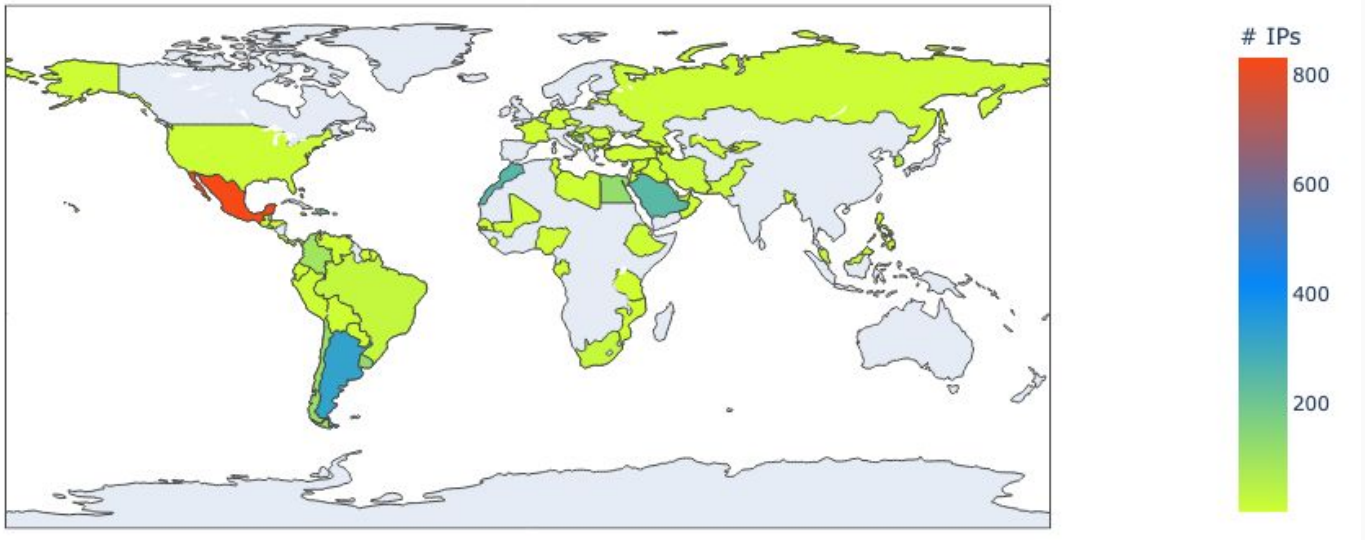
Service Information

- In use by SmokeLoader (botnet that was taken down last year).
- In 2024
  - 193 Domains and 42 nameservers
  - 2.9k unique IPs (residential)
- Based on self-signed cert, likely to be SandiFlux/Dark Cloud
- Most domains used for C2 or droppers
  - SmokeLoader, Amadey, LummaC2
- Used for carding websites, phishing, hosting data leaks



Service Information

- 82% of IPs from 10 countries
  - Previous research showed a focus in Eastern Europe.



Call for Action

- Anyone follows this service?
- Is it indeed SandiFlux/Dark Cloud?
- Is it associated with a known dark market service?
- What malware is behind it? Most recent sample from 2017, still the same?

@jcfg_ infosec.exchange/@jcfg @jcfg.re