## Identifying Laplas Infrastructure Using Shodan and Censys

embee-research.ghost.io/laplas-clipper-infrastructure/

Matthew May 18, 2023

#### intel

Quick identification of Laplas infrastructure by utilising Shodan and Censys.

Various queries for locating potential Laplas Infrastructure. Based on an IP found in a Laplas sample from Malware Bazaar.

The full list can be found at the end of post.

#### Link to Sample

SHA256: 825b0080782dee075f8aac11c3a682f86c5d3aa5462bd16be0ed511a181dd7ba

Links to relevant existing research by <u>OALABS</u> and <u>Chris Duggan</u>. Chris in particular has some work that is very similar to this.

```
public static string Destination
{
    [CompilerGenerated]
    get
    {
        return "45.159.189.105";
    }
}
```

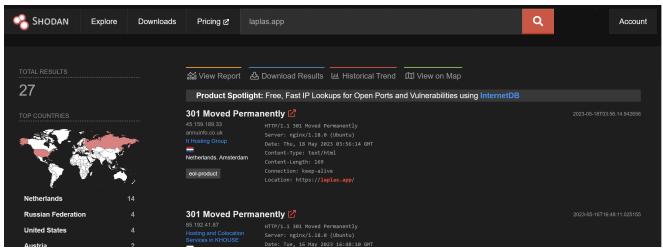
Searching this ip in shodan reveals a server that redirects to <a href="https://laplas[.].app">https://laplas[.].app</a>

```
## 80 / TCP 1

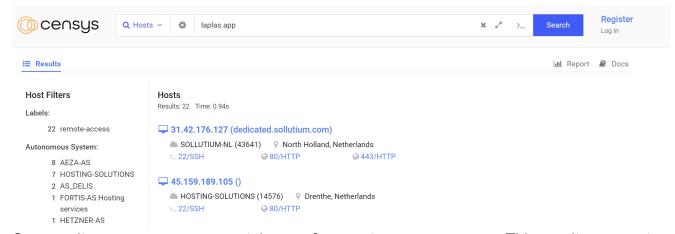
nginx 1.14.2

HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.2
Date: Sat, 06 May 2023 10:44:42 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: https://laplas.app/
```

Searching laplas.app reveals 27 servers. Each server appears to be a redirector to the main Laplas site.



Searching laplas.app in Censys reveals 22 servers. Two of which were not in the original Shodan list.



One result 31.42.176[.]127 contains a reference to CN=Laplas.app. This result appears to be the primary server.

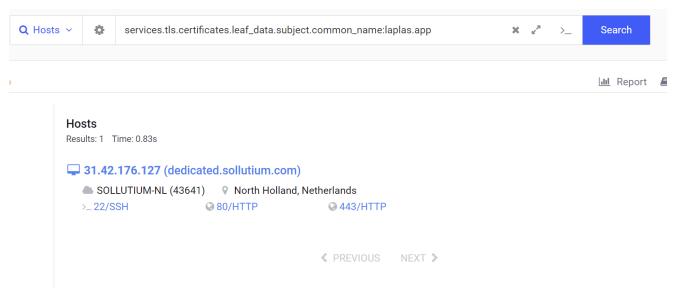
#### **Leaf Certificate**

#### b286e1b6f2d8ea2c0646f39cde7c844b40872769dc844d487e78f80afd1135d8

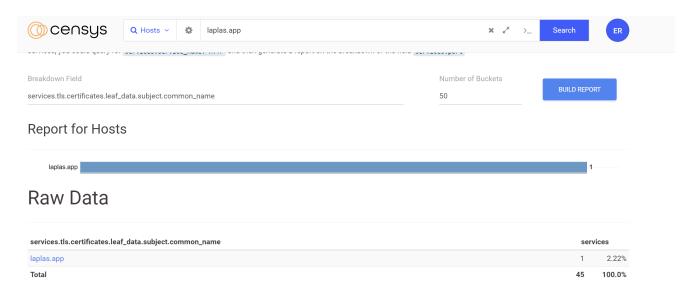
CN=laplas.app

C=US, O=Let's Encrypt, CN=R3

Searching for the common name of laplas.app does not reveal additional infrastructure. Only the initial result of 31.42.176[.]127 was found.



Of the 22 results with Censys, No other common names were available that could be used for pivoting.



Only one Jarm hash was available. This was a common Jarm fingerprint with around 205K results and hence was not useful for pivoting.

services.jarm.fingerprint=15d3fd16d29d29d00042d43d000000fe02290512647416dcf0a4

# Report for Hosts Cr(0a400ccbc0b6b) Raw Data services.jarm.fingerprint 15d3fd16d29d29d000042d43d000000fe02290512647416dcf0a400ccbc0b6b 1 2.22% Total 45 100.0%

### **Complete List of Potential Laplas Stealer Infrastructure**

Complete list of IP's based on searches for laplas.app in both Shodan and Censys.

31.42.176.127 37,220,87,60 45.81.243.208 45.159.188.109 45.159.188.158 45.159.189.33 45.159.189.105 65.109.140.234 78.153.130.208 79.137.195.205 79.137.199.252 80.85.241.66 85.192.40.252 85.192.41.87 89.23.97.128 89.185.85.79 95.214.27.252 104.193.254.40 104.193.255.50 163.123.142.220 176.113.115.25 185.106.92.104 185.174.137.94 185.209.161.89 185.213.208.247 185.223.93.251 193.188.23.86 195.133.75.43

212.113.106.172