1 IP address
2 country locations

Introducing Geolocus database

https://www.geolocus.io/

Patrice Auffret, founder & CTO

patrice.auffret@onyphe.io

What is ONYPHE?

- **ONYPHE** - Cyber Defense Search Engine

- Technical data collection
  - Internet connected objects & URLs, Dark Web
  - Threat feeds
  - Passive DNS
  - **Reverse Whois**
  - Certificate Transparency Logs
  - Online copy/paste solutions
  - Internet background noise

- Searchable from Web site and REST API
  - **Attack Surface Discovery**
  - **Attack Surface Management**

ONYPHE

The Russification of Ukrainian IP Registration

https://www.kentik.com/blog/the-russification-of-ukrainian-ip-registration/ - February 23, 2023

Summary

In this article, Doug Madory uncovers the little-known "Russification" of Ukrainian IP addresses — a phenomenon that complicates the task of internet measurement and impacts Ukrainians connecting to the internet using IP addresses suddenly considered Russian.

registration changes taking place in Crimea following the Russian annexation in March 2014.

Last summer we teamed up with the New York Times to analyze the re-routing of internet service to Kherson, a region in southern Ukraine that was, at the time, under Russian occupation. In my accompanying blog post, I described how that development mirrored what took place following Russia's annexation of Crimea in 2014.

Along with the Russian-held parts of eastern Ukraine, these regions have experienced a type of *Russification*, an assimilation where the Ukrainian residents of these regions have been forced to adopt all things Russian: language, currency, telephone numbers, and, of course, internet service.

Using a novel utility made available by RIPE NCC, we have identified dozens of changes to registrations, revealing another target of this Russification effort: the geolocation of Ukrainian IP addresses.

Whois records vs tracerouting

- **Logical** geolocation can be found from **whois** records
  - Country field
- **Physical** geolocation can be found from **tracerouting**
  - Uncover « last-hop » geolocation
- **Both information can be useful**
  - **Logical country geolocation**
  - **Physical country geolocation**

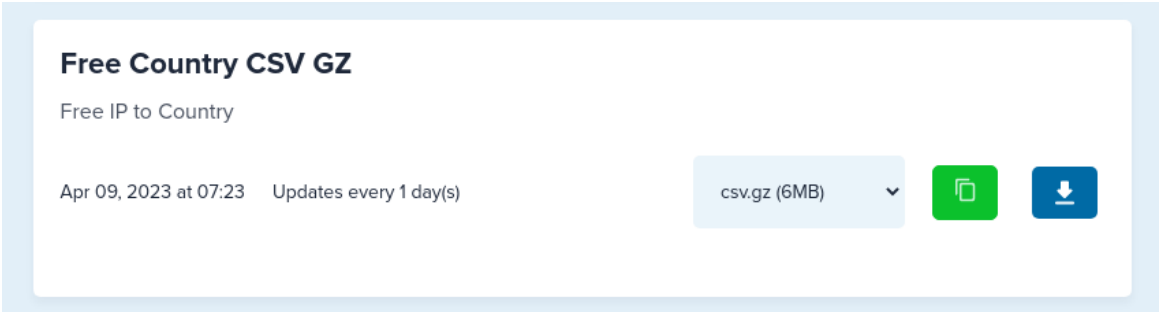
1 IP address, 2 country locations

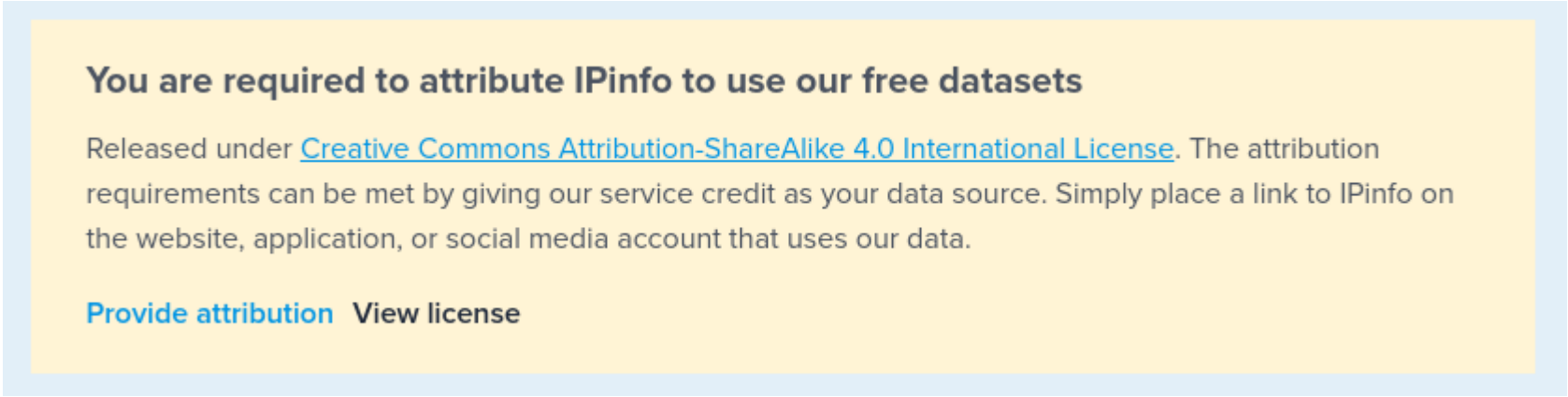
No geolocation database gives **both***

* Until Geolocus: https://www.geolocus.io/

How our database is built?

- Our idea surged from **ipinfo.io**
  - They provide **physical** location for free
- Correlated with **our whois collected data**





Physical IP address data powered by https://ipinfo.io, all other fields powered by Geolocus.

Demonstration

- 178.158.128.0/18
- 178.219.192.0/20
- 95.215.48.0/22
- 91.194.162.0/23
- 46.35.224.0/20

- **Physical: UA**
- **Logical: RU**

ONYPHE

Conclusion

- Geolocus is an IP to 2-country geolocation database
  - Physical & logical locations
- **You decide which one suits your needs**
- **Side-project from ONYPHE**
  - Will be integrated in ONYPHE soon
- Free as in beer – no license
  - https://www.geolocus.io/

Merci.

Twitter: @ONYPHE, @PatriceAuffret

Register: https://www.onyphe.io/signup

Pricing: https://www.onyphe.io/pricing

Github: https://github.com/onyphe

ONYPHE