How Rogue ISPs Tamper With Geofeeds

medium.com/@DCSO_CyTec/how-rogue-isps-tamper-with-geofeeds-4dbc38db4123

DCSO CyTec Blog March 20, 2024

DCSO CyTec Blog

--

Precise geolocation information for IP addresses has emerged from a niche requirement to a ubiquitous demand. While the country an IP address is (allegedly) related to has long been used for applications such as network traffic distribution and coarse geoblocking, today, state-, city- and sometimes even district-level geolocation information is crucial for modern security measures, such as fraud detection. Data brokers, advertisers, defenders, and investigators alike are interested in having precise and up-to-date information on the *physical* location of an IP address at their disposal. The demand for such information has nurtured an entire industry, with US-based vendor MaxMind probably being the most commonly referred to source for geolocation information.

Photo by on

However, a steady demand in geolocation information beyond a country-level has incentivized efforts to allow ISPs to propagate such information independently, perhaps further driven by MaxMind's EULA changes for its free GeoLite2 databases in 2019, which has caused problems particularly among the open-source community.

A result of this development is IP Geolocation Feeds, commonly abbreviated as "geofeeds." By publishing these, ISPs can ensure that geolocation database vendors, among others, are more likely to learn about and subsequently return correct information for the IP networks under an ISP's control.

Unfortunately, threat actors are leveraging geofeeds as well, and have been observed publishing forged information, presumably with the objective of circumventing access control measures (such as country-level geoblocking) and hampering investigations. This blog post strives to shed light on a particularly noteworthy example, which also serves as a case study for discussing the viability of geofeeds as OSINT pivot points. Furthermore, countermeasures for defenders and investigators are suggested.

Blog post authored by .

A Primer On Geofeeds

Specified in RFC 8805, IP Geolocation Feeds — commonly abbreviated as "geofeeds" — allow ISPs to distribute information on the physical location of IP networks, consisting of country, region/state, city, and ZIP code. Such information can then be parsed and (comparatively) easily included in geolocation databases for improved accuracy. A separate internet standard, RFC 9092, discusses how to discover and verify geofeeds at scale in a structured fashion, such as in Regional Internet Registry (RIR) databases.

It is worth noting that RIR databases have long allowed the allocation of a country to IP network and Autonomous System (AS) objects, as the following example from the RIPE database shows:

```
inetnum:        185.183.126.0 - 185.183.126.255netname:        Infrastructurecountry:
DEadmin-c:        DCSO-RIPEtech-c:         DCSO-RIPEstatus:         LIR-PARTITIONED
PAmnt-by:         DCSO-MNTcreated:        2020-08-28T08:45:53Zlast-modified:  2020-
08-28T08:45:53Zsource:         RIPE
```

However, it may not always be clear whether the "country" database field refers to the country a network is *physically* located in, or the *jurisdiction* that applies to it. (Both are Germany in the above example.) Consequently, many geolocation database vendors who incorporate country-level information from RIR databases abstain from clarifying this aspect as well, which often causes geolocation database users to be overly confident in the understanding of database outputs.

Aside from that, RIR database schemes commonly do not allow for the machine-digestible publication of more precise geolocation information, such as the involved state or city. Assessing these by examining routing information, network latency triangulation, and other technical measures is often, but not always, feasible and is considerably more resource-intensive than parsing geofeeds and alike databases. While advertising and tracking networks may be able to correlate IPs with precise geolocation information made available from end-user devices (i.e., through GPS sensors and WiFi network mapping), collecting such information is a rather privacy-invasive measure.

An arbitrary example of a geofeed reference in RIR databases may look like this (note the "geoloc" field, which — unrelated to geofeeds — contains geographic coordinates on the physical location of this IP network):

```
inetnum:        5.149.224.0 - 5.149.239.255netname:        DE-R-KOM-20120717country:
DEgeoloc:         49.014042 12.127519geofeed:        https://geofeed.r-
kom.de/geofeed.csvorg:            ORG-RA3-RIPEadmin-c:        RKOM-RIPEtech-c:
RKOM-RIPEstatus:         ALLOCATED PAmnt-by:         RKOM-MNTmnt-by:         RIPE-
NCC-HM-MNTcreated:        2019-12-20T12:47:47Zlast-modified:  2022-10-
20T06:04:14Zsource:         RIPE
```

The CSV file will then contain further information, such as in this case:

```
5.149.224.0/20,DE,DE-BY,Regensburg,
```

This allows geolocation database vendors to easily locate 5.149.224.0/20 in the city of Regensburg, Bavaria, Germany. At the time of writing, DCSO has no reason to question this particular geolocation information.

Eygelshoven, Edison, or Paris? — A Case Study

However, not all geofeed use-cases are this benign, as the case of AS203168 (allocated to "Constant MOULIN") shows: at the time of writing, five out of six IPv4 prefixes announced by this AS contain geofeed information, such as:

```
inetnum:        45.88.90.0 - 45.88.90.255netname:        CONSTANTMOULINdescr:
Constantmoulinorg:            ORG-CM304-RIPEcountry:        FRgeofeed:
https://raw.githubusercontent.com/geofeeds/geofeed/main/geofeed.csvadmin-c:
ACRO54823-RIPEtech-c:         ACRO54823-RIPEabuse-c:        ACRO54823-RIPEmnt-lower:
personal-ip-mntmnt-routes:     personal-ip-mntmnt-domains:    personal-ip-mntstatus:
ASSIGNED PAmnt-by:         MNT-NETERRAcreated:        2024-02-09T14:35:37Zlast-
modified:  2024-03-05T10:17:23Zsource:         RIPE
```

This geofeed URL, at the time of writing, returns:

```
193.222.96.0/24,NL,NL-LI,Eygelshoven,87.120.84.0/24,US,US-
NJ,Edison,45.128.96.0/24,US,US-NJ,Edison,45.88.90.0/24,FR,FR-
75,Paris,194.48.251.0/24,FR,FR-75,Paris,
```

This suggests that 45.88.90[.]0/24 is physically located in or near Paris, France. Indeed, global routing information and network latency triangulation efforts carried out by DCSO corroborate this information.

However, this assessment does not hold true for all entries of this geofeed, particularly not for 45.128.96[.]0/24 and 87.120.84[.]0/24, both allegedly located in or near Edison, New Jersey, USA. Firstly, it is noteworthy that the RIPE database objects for both networks list "FR" (France) as the country code (both output have been trimmed for brevity reasons):

```
inetnum:        45.128.96.0 - 45.128.96.255netname:        CONSTANTMOULINdescr:
Constantmoulingeofeed:
https://raw.githubusercontent.com/geofeeds/geofeed/main/geofeed.csvcountry:
FR<snip>

inetnum:        87.120.84.0 - 87.120.84.255netname:        BG-NETERRAIP-
20050712country:        FRorg:            ORG-NL38-RIPEadmin-c:        ACRO54823-
RIPEtech-c:         ACRO54823-RIPEabuse-c:        ACRO54823-RIPEstatus:
ALLOCATED PAgeofeed:
https://raw.githubusercontent.com/geofeeds/geofeed/main/geofeed.csv<snip>
```

However, as mentioned above, the "country" could also refer to the jurisdiction that applies to these networks—which would prompt questions as well, given that the postal addresses provided for AS203168 in general and both networks in particular refer to Dinant, a city in the Belgian province Namur.

At the time of writing, 45.128.96[.]0/24 is routed via AS49581 ("Ferdinand Zink trading as Tube-Hosting," according to the RIPE database), an ISP offering VPS, VDS, and colocation services in the SkyLink datacenter, located in Eygelshoven, the Netherlands. DCSO was unable to discover any presence of this ISP in the USA; indeed, the following router appearing in traceroute outputs for this network corroborates the hypothesis of this /24 being located in Eygelshoven. However, it is worth noting that "EGH" does not appear to be the IATA or UN/LOCODE code allocated to Eygelshoven (both IATA and UN/LOCODE are frequently used for referring to physical locations).

```
ae4.1129-1.cr1.egh.as49581.net (80.91.223.18)
```

BGP routing information for this /24 also contain SkyLink's AS (AS44592), further corroborating DCSO's aforementioned hypothesis that this network is neither physically located in France (according to its RIPE database record) nor in the USA (according to its geofeed):

```
45.128.96.0/24       4608 7575 199524 44592 49581 203168 203168
```

As far as 87.120.84[.]0/24 is concerned, it appears to be routed via AS399486 (12651980 CANADA INC.) at the time of writing. According to its website, this ISP offers dedicated server and colocation offerings in data center facilities in Montreal, Canada, as well as

Edison, USA. However, DCSO was unable to conclusively assess in which of these facilities 87.120.84[.]0/24 is physically located, and it remains unclear why the network's RIPE database object lists France in its "country" attribute.

It is worth mentioning that all prefixes announced by AS203168, as well as the Autonomous System itself, are listed in Spamhaus DROP lists at the time of writing, suggesting a poor reputation of this ISP:

> The Spamhaus DROP lists consist of netblocks that are leased or stolen by professional spam or cyber-crime operations, and used for dissemination of malware, trojan downloaders, botnet controllers, or other kinds of malicious activity.

DCSO was unable to discover a website publicly mentioning services hosted by AS203168, which leads to the suspicion that this ISP does not advertise and sell its services through public-facing websites. 194.33.191[.]0/24, a prefix currently announced by this Autonomous System, was previously in use by AS211252, allocated to Delis LLC, a now-defunct bulletproof hoster operating out of a data center owned by Dutch ISP Serverion BV.

According to news reporting, the aforementioned SkyLink data center has previously come under scrutiny by Dutch law enforcement authorities in conjunction with illegal IPTV streaming, culminating in a raid carried out by the Netherlands' fiscal intelligence unit (FIOD) on March 23, 2023.

OSINT Pivot Potential of Geofeeds

It is well understood that, from an OSINT perspective, any kind of database whose edit history can be publicly retrieved — which often is the case for RIR databases — has the potential of holding a wealth of information suitable for enabling or proliferating investigations.

In the case of geofeeds, this may also apply to the content of the geofeed itself, particularly if it is provided via a source code repository. In the case of AS203168, combining both historical RIPE database information and metadata retrieved from the involved Git repositories unveils further information on entities associated with or controlling AS203168.

First, historical versions of RIPE database objects of the involved prefixes contain different geofeed URLs (output trimmed for brevity):

```
inetnum:        45.88.90.0 - 45.88.90.255netname:        CONSTANTMOULINdescr:
Constantmoulinorg:            ORG-CM304-RIPEcountry:        FRgeofeed:
https://raw.githubusercontent.com/pfcloud-io/geofeed/main/geofeed.csv<snip>
```

This suggests a certain degree of involvement by German Pfcloud UG in the operation of AS203168. On the same day when the RIPE database object for 45.88.90[.]0/24 was last updated to include aforementioned, more unobtrusive geofeed URL (March 5, 2024), a

variety of networks were deleted via a Git commit in the geofeed GitHub repository that Pfcloud maintains.

```
commit 22722a610a1ecc6548cb0b539aca5c5d77fe9e72 (HEAD -> main, origin/main,
origin/HEAD)
Author: TeamAggro (~Steve) <49125036+TeamAggroDEV@users.noreply.github.com>
Date:   Tue Mar 5 09:56:26 2024 +0100


    Update geofeed.csv

diff --git a/geofeed.csv b/geofeed.csvindex 7de625e..d6aaf67 100644---
a/geofeed.csv+++ b/geofeed.csv@@ -8,10 +8,6 @@ 147.78.102.0/24,NL,NL-LI,Eygelshoven,
87.121.69.0/24,GB,GB-LND,London, 87.121.58.0/24,NL,NL-
LI,Eygelshoven,-193.222.96.0/24,NL,NL-LI,Eygelshoven,-87.120.84.0/24,US,US-
NJ,Edison,-45.128.96.0/24,US,US-NJ,Edison,-45.88.90.0/24,FR,FR-75,Paris,
2a05:b0c6:a000::/39,US,US-AZ,Phoenix, 2a05:b0c6:a200::/39,DE,DE-BE,Berlin,
2a05:b0c6:a400::/39,GB,GB-LND,London,
```

A Git commit made to the "geofeeds" GitHub repository only 34 seconds prior not only includes all four IPv4 networks that were deleted from Pfcloud's GitHub repository, but also lists the same author, "TeamAggro (~Steve)". DCSO assesses that this likely is a reference to a Hull, UK-based company named Aggros Operations Ltd., which surfaced in historical RIPE database records for prefixes announced by AS203168, as does a RIPE handle allocated to Pfcloud ("pfcloud-mnt").

Noteworthy, the timestamp of both Git commits lists "+0100" as a timezone, which (weakly) indicates the involved computer's clock being aligned to Central European Time (CET) rather than Greenwich Mean Time (GMT), which would be used by UK-based systems. The British Summer Time (BST), which would also result in "+0100", only commences on March 31 in 2024, several weeks after the Git commits have taken place.

```
commit 358614d3c919471d8bba6ce31f9f9583bda3adba (HEAD -> main, origin/main,
origin/HEAD)
Author: TeamAggro (~Steve) <49125036+TeamAggroDEV@users.noreply.github.com>
Date:   Tue Mar 5 09:55:52 2024 +0100


    Create geofeed.csv

diff --git a/geofeed.csv b/geofeed.csvnew file mode 100644index 0000000..63ec36f---
/dev/null+++ b/geofeed.csv@@ -0,0 +1,5 @@+193.222.96.0/24,NL,NL-
LI,Eygelshoven,+87.120.84.0/24,US,US-NJ,Edison,+45.128.96.0/24,US,US-
NJ,Edison,+45.88.90.0/24,FR,FR-75,Paris,+194.48.251.0/24,FR,FR-75,Paris,
```

```
inetnum:        45.88.90.0 - 45.88.90.255
netname:        CONSTANTMOULIN
descr:          Constantmoulin
org:            ORG-CM304-RIPE
country:        FR
geofeed:        https://raw.githubusercontent.com/pfcloud-io/geofeed/main/geofeed.csv
admin-c:        AA39986-RIPE
tech-c:         AA39986-RIPE
mnt-lower:      aggrosoperations-mnt
mnt-routes:     aggrosoperations-mnt
mnt-domains:    aggrosoperations-mnt
status:         ASSIGNED PA
mnt-by:         MNT-NETERRA
created:        2024-02-09T14:35:37Z
last-modified:  2024-02-09T14:35:37Z
source:         RIPE


organisation:   ORG-CM304-RIPE
org-name:       Constant MOULIN
country:        BE
org-type:       OTHER
address:        RUE SAINT-JACQUES 108/3 5500 DINANT
abuse-c:        ACRO54823-RIPE
mnt-ref:        mnt-fr-scalynet-1
mnt-ref:        mnt-neterra
created:        2022-08-23T16:10:16Z
last-modified:  2023-12-19T10:27:14Z
source:         RIPE # Filtered
mnt-by:         mnt-fr-scalynet-1
mnt-by:         be-constantmoulin-mnt


role:           Administration
address:        Aggros Operations Ltd, c/o COCENTER, Koppoldstr. 1, 86551 Aichach,
Germany
nic-hdl:        AA39986-RIPE
mnt-by:         aggrosoperations-mnt
created:        2022-09-25T15:51:13Z
last-modified:  2023-01-27T17:05:24Z
source:         RIPE # Filtered


% Information related to '45.88.90.0/24AS203168'

route:          45.88.90.0/24origin:         AS203168created:        2024-02-
10T12:33:50Zlast-modified:  2024-02-10T12:33:50Zsource:         RIPEmnt-by:
pfcloud-mnt
```

In this case, the geofeed URL is suitable for usage as an OSINT pivot point and resembles a crucial information breadcrumb for linking Pfcloud UG and Aggros Operations Ltd. to each other and to the operational aspects of AS203168.

Similar to other investigative use-cases, GitHub repositories used for geofeed URL hosting may allow detailed insights into the history of an ISP, (alleged) physical facilities used by it, related personas or GitHub accounts, OpSec mistakes made by involved entities, and attempts to cover up such mistakes.

Potential Risks Induced By Geofeed Processing

In contrast to RIR databases, geofeed URLs carry several potential risks that geolocation database vendors and investigators alike may wish to keep in mind:

- While the file integrity of the vast majority of publicly downloadable RIR databases can be verified through cryptographic signatures, such information commonly is not available for geofeeds (, specifies authentication of geofeed data, however, DCSO has rarely observed in-the-world deployment of this authentication scheme).
- Similarly, while , mandates HTTPS as a protocol for publishing and retrieving geofeed URLs, the usage of other security measures such as or is not even discussed by this RFC, leaving geofeed downloads at risk of being silently manipulated by (more sophisticated) threat actors capable of issuing trusted X.509 certificates for arbitrary FQDNs on the fly.
- Particularly in cases where geofeed URLs are hosted on infrastructure under direct control by the involved ISP, different geofeed content may be presented to different clients, in order to deliberately “inject” certain data into certain databases or security solutions. This may be enabled by custom tooling revealing itself through unique HTTP User-Agent headers or through conducting geofeed downloads from certain IP addresses that can be attributed to organizations of interest.
- Especially in the case of manual investigations, an ISP may also harvest such data to achieve a better understanding of ongoing investigations, as well as individuals or organizations conducting such investigations. In order not to compromise the investigator’s OpSec, exercising the same caution for accessing geofeed URLs as other resources controlled by an ISP remains crucial.

Conclusion

Geofeeds enable ISPs to propagate precise geolocation information on their IP networks in a decentralized, independent, and machine-digestible fashion, thus allowing geolocation database vendors to display such information with a greater likelihood (and reducing the necessity of such vendors to procure precise location data from privacy-invasive sources).

However, as the example of AS203168 demonstrates, geofeed contents may be worth approaching with caution. By deliberately injecting inaccurate information, rogue ISPs may seek to (selectively or opportunistically) poison databases created by geolocation and security vendors, and attempt to hamper manual investigations. DCSO therefore recommends geolocation vendors and defenders alike reconsider processing geofeeds published by ISPs with a poor reputation, and resort to filtering based on Autonomous System information rather than country-based schemes (“geoblocking”) for improved accuracy. This is crucial, as it is often trivial for a threat actor to gain access to an IP address geolocated within a certain country, and countries hosting a significant fraction of today’s popular internet services (which includes the Netherlands) de facto cannot be geoblocked without causing an unacceptable amount of false positives.

Should geoblocking be considered viable by defenders regardless, they may seek technical solutions to assess the likelihood of geolocation information having been forged by questionable ISPs. Should such an assessment return a high likelihood of grossly inaccurate information, affected network traffic should be subject to further scrutiny.

Especially if hosted by source-code tracking infrastructure, such as GitHub repositories, geofeeds may also pose highly interesting OSINT pivot points, allowing investigators to easily unveil a greater fraction of an ISP’s operation and its historical development. In order to not compromise OpSec though, geofeed URLs should be accessed with the same precautionary measures in place for interacting with other resources controlled by questionable ISPs.

Related Information

Live Spamhaus SBL/DROP listings concerning prefixes announced by AS203168 at the time of writing:

-
-
-
-
-
-

Live Spamhaus ASN-DROP listing concerning AS203168 at the time of writing:


```
{"asn":203168,"rir":"ripencc","domain":"stellar-
group.fr","cc":"BE","asname":"unknow"}
```