Adversary in the middle (AiTM), BEC, MITRE ATT&CK T1557

Expand the visualization to geolocation map with Azure Data Explorer

1. Summarize the countries that authenticated to the OfficeHome application for each user and list any uncommon or untrusted countries.
2. Track the user account with multiple country logins and list the associated ***"Country," "Latitude,"*** and **"Longitude"** data.
3. Visualize suspicious access to the user account on a geolocation map using **Azure Data Explorer**.

```
AADSignInEventsBeta
| where Timestamp > ago(7d)
| where ApplicationId == "4765445b-32c6-49b0-83e6-1d93765276ca"
| where ClientAppUsed == "Browser"
| where LogonType has "interactiveUser"
| summarize Countries = make_set(Country) by AccountObjectId, AccountDisplayName
```

```
AADSignInEventsBeta
| where Timestamp > ago(7d)
| where ApplicationId == "4765445b-32c6-49b0-83e6-1d93765276ca"
| where ClientAppUsed == "Browser"
| where LogonType has "interactiveUser"
| where AccountUpn == "malware@xxxxxxx.onmicrosoft.com"
```

```
datatable (Latitude:real, Longitude:real, Country:string, Timestamp:datetime)[
35.69628,139.7386,"JP",datetime(2023-07-03),
22.24831,114.1524,"HK",datetime(2023-07-03),
38.73078,-78.17197,"US",datetime(2023-07-07),
51,9,"DE",datetime(2023-07-04),
47.791939,264.887962,"US",datetime(2023-07-03),
31.289113,261.269105,"US",datetime(2023-07-04),
45.415804,262.925967,"US",datetime(2023-07-05),
38.934844,249.760892,"US",datetime(2023-07-06)
]
| project Longitude, Latitude, Timestamp
| render scatterchart with (kind = map)
```

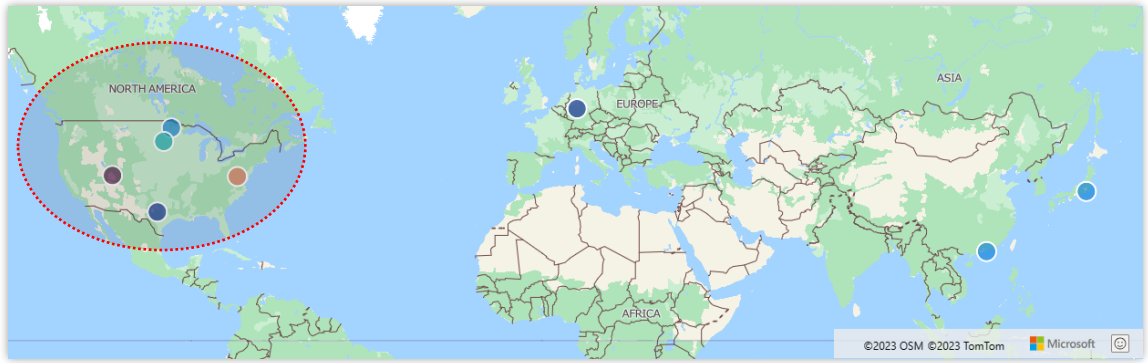
- Kusto Desktop Explorer
- Azure Data Explorer

AccountObjectId	AccountDisplayName	Countries
4a12803	Malware M365D	["JP","DE","HK","US"]
0668ad9	Steve M365D	["JP"]
1e758c5	Darol M365D	["JP"]

1 of 17 selected | Search

Country	Latitude	Longitude
JP	35.69628	139.7386
HK	22.24831	114.1524
DE	51	9

AccountUpn
malware@ .onmicrosoft.com
IPAddress
20.55.57.144
Country
US
Latitude
38.73078
Longitude
-78.17197



Initial Access | Execution | Persistence | Privilege Escalation | Credential Access | Collection | Exfiltration | Impact

Geospatial data visualizations | Microsoft Learn
From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | Microsoft Security Blog