# Hybrid-Analysis.com “Threat Map”

Objective is to create a “threat map” that is similar to <http://map.norsecorp.com/> or <https://threatmap.fortiguard.com/> based on data from the feed at <https://www.hybrid-analysis.com/feed?json>. The idea is to create a fullscreen, standalone application that can be made available as a marketing effort. The first version will be very simple and consist of two aspects:

* “detonation” animations at the longitude/latitude locations found in the “hosts\_geo” JSON array of the feed (see above)
* a constantly scrolling list of single rows that is taken from the “et\_alerts” 🡪 “actions” 🡪 “description” field of the feed

## Specification/Requirements

* Create a worldmap with leaflet that allows applying latitude/longitude values (e.g. using “darkmatternolabels” provider (<https://leaflet-extras.github.io/leaflet-providers/preview/>):
* Build an animation for the “detonation” (aniticpating different colors, e.g. green/orange/red that resemble different severities)
* All available JSON objects at <https://www.hybrid-analysis.com/feed?json> resemble one “cycle”. One “cycle” is defined as X seconds (e.g. 30). During this period of time, we want to animate all detonations (i.e. each “hosts\_geo” array element entry of all JSON objects in the global feed array)
* The view of the threat map should be “infinite”, i.e. whenever one cycle has completed, it just rerstarts
* The code is built to be generic, as we will add more fields for the “description” at a later point. Also, the input data parsing and rendering parts should be separated, as we will most likely have different data input sources eventually
* Add a “blue/green neon color” as the country border drawings (similar to the norsecorp map; see above)
* All colors/settings (e.g. cycle length, animation speeds, etc.) should be configurable from a settings file

## Example JSON Data Object

Note: the yellow highlighted data is the to-be-parsed parts

"md5": "e909c5aa7a3a6cff67d3af71da54712a",

"sha1": "e1865b900ab1e516c0e1cf3ee5bbbef7374735d8",

"sha256": "3b0bcbebb410c9733cca953e45427273dcf2bae8c1005708270e5f088fac42db",

"tags": [

"neutrino"

],

"isinteresting": false,

"analysis\_start\_time": "2017-07-16 19:04:31",

"threatscore": 100,

"threatlevel": 2,

"avdetect": 68,

"isunknown": false,

"vxfamily": "Trojan.Generic",

"submitname": "DiscordSpyTool.exe",

"isurlanalysis": false,

"size": 219648,

"type": "PE32 executable (GUI) Intel 80386 Mono\/.Net assemb ...",

"domains": [

"ns.dotbit.me",

"ns1.any.dns.d0wn.biz",

"onyx.deepdns.cryptostorm.net",

"ns1.random.dns.d0wn.biz",

"alors.deepdns.cryptostorm.net",

"xzojcwac.com"

],

"hosts": [

"107.161.16.236",

"62.117.121.194",

"198.251.86.12",

"178.17.170.133",

"185.145.131.235"

],

"hosts\_geo": [

{

"ip": "107.161.16.236",

"lat": "32.8407",

"lon": "-83.6324",

"cc": "US"

},

{

"ip": "62.117.121.194",

"lat": "55.7386",

"lon": "37.6068",

"cc": "RU"

},

{

"ip": "198.251.86.12",

"lat": "41.1034",

"lon": "-104.9059",

"cc": "US"

},

{

"ip": "178.17.170.133",

"lat": "47.0056",

"lon": "28.8575",

"cc": "MD"

},

{

"ip": "185.145.131.235",

"lat": "52.3824",

"lon": "4.8995",

"cc": "ZZ"

}

],

"compromised\_hosts": [

"107.161.16.236",

"62.117.121.194",

"198.251.86.12",

"178.17.170.133",

"185.145.131.235"

],

"et\_alerts": [

{

"destip": "217.198.115.56",

"destport": "80",

"protocol": "TCP",

"action": {

"signatureid": "2008350",

"signaturerev": "7",

"severity": "1",

"category": "Potential Corporate Privacy Violation",

"description": "ET POLICY Autoit Windows Automation tool User-Agent in HTTP Request - Possibly Hostile"

}

},

{

"destip": "217.198.115.56",

"destport": "80",

"protocol": "TCP",

"action": {

"signatureid": "2019935",

"signaturerev": "2",

"severity": "1",

"category": "A Network Trojan was detected",

"description": "ET TROJAN AutoIt Downloading EXE - Likely Malicious"

}

},

{

"srcip": "217.198.115.56",

"destport": "57900",

"protocol": "TCP",

"action": {

"signatureid": "2018959",

"signaturerev": "3",

"severity": "1",

"category": "Potential Corporate Privacy Violation",

"description": "ET POLICY PE EXE or DLL Windows file download HTTP"

}

},

{

"destip": "217.198.115.56",

"destport": "80",

"protocol": "TCP",

"action": {

"signatureid": "2008350",

"signaturerev": "7",

"severity": "1",

"category": "Potential Corporate Privacy Violation",

"description": "ET POLICY Autoit Windows Automation tool User-Agent in HTTP Request - Possibly Hostile"

}

}

],