TLP:AMBER – MELANI BLAU

MELANI BGP

Version: v1.0
Date: 2019-09-23

Introduction

MELANI/GovCERT provides a BGP feed to the operators of national Critical Infrastructures (CI) in Switzerland. The goal of the feed is to avoid infections or to limit damage in the case of an infection by blocking (null-routing) connections to botnet Command and Control Servers (C&C).

We use carefully selected sources as input, namely:

- MELANI Botnet List (MELBL[1])
- Extract from Feodo Tracker[2] (Emotet and TrickBot)

This manual describes how to peer with MELANI.

Available BGP Communities

MELANI offers the following BGP communities (“lists”) described below. You are free to choose which communities you would like to apply on your network.

MELBL_IP (65351:1000)

This community is **maintained manually** (4-eyes principal) by GovCERT.ch and contains IPv4 addresses (/32) that we strongly believe are operated by bad actors for the sole purpose of hosting botnet C&C servers. Null routing (blocking) IP addresses announced on this community should cause **no false positives**.

EMOTET_IP (65351:2000)

This community is **maintained automatically** and contains IPv4 addresses (/32) that are hosting an **active** Emotet or TrickBot botnet C&C. We check several times per hour in an automated way if such a botnet C&C is still active. If this is the case, the IPv4 address gets immediately removed from the community (unblocked).

As some Emotet and TrickBot C&Cs are hosted on compromised machines (usually compromised CPE devices), nullrouting IP addresses announced by this community **may cause**

[1] See separate service description of MELBL
[2] https://feodotracker.abuse.ch/

false positive. However, we believe that the false positive rate should be very low as many of such C&Cs are hosted in Latin America.

Router Configuration

Overview

Item	Value
IP Adresse	5.148.169.122
Port (Standard BGP)	179/TCP
AS number	AS65351
Community MELBL	1000
Community Emotet/Trickbot	2000

Step-By-Step Guide

Please note that:

- We recommend you to not execute any of the commands mentioned in this document unless either you have tested them in a test environment, or you know exactly what you are doing!
- Some commands may vary depending on your router vendor

First of all, you need to define a null-route target if you have not already done so. You do this using the following command:

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Note: You should use a private IP address here (like 192.0.2.1). Do not use a public IP address unless you know what you are doing.

Now, we need to create the BGP communities. Please refer to chapter “Available BGP Communities” for further information about the available BGP communities and their purpose.

```
ip community-list standard MELBL_IP permit 65351:1000
ip community-list standard EMOTET_IP permit 65351:2000
```

The following command will prevent that you announce your BGP routing table to MELANI:

```
ip prefix-list NONE seq 5 deny 0.0.0.0/0
```

Create a route map for the BGP communities we just created. Depending on the BGP communities you would like to apply, this configuration may vary (see “Available BGP Communities”):

```
route-map MELANI permit 1000
description MELBL_IP
match community MELBL_IP
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive route-map MELANI
```

```
permit 2000

description EMOTET_IP
match community EMOTET_IP
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive
```

Finally, you have to configure your router to peer with our router:

```
router bgp <your-AS-number>
neighbor 5.148.169.122 remote-as 65351
neighbor 5.148.169.122 description MELANI
neighbor 5.148.169.122 maximum-prefix 250 80
neighbor 5.148.169.122 update-source <your-routers-ip-address-or-
interface>
neighbor 5.148.169.122 ebgp-multihop 255 address-family ipv4
unicast
neighbor 5.148.169.122 activate
neighbor 5.148.169.122 prefix-list NONE out
neighbor 5.148.169.122 route-map MELANI in
```

We strongly suggest adding additional filters that ensure that:

- only /32 routes are accepted
- no null accidental null routing may happen of critical systems of yours or your customers.

Once the configuration on your router is completed, please send an email containing the following information to outreach@govcert.ch:

- IPv4 address of your Router
- Your AS Number

Disclaimer

- The use of this service is subject to MELANI's standard NDA
- MELANI cannot assume any liability for the completeness or correctness of the service described herein or the data/information it contains.
- MELANI cannot be held liable for any damage or false positives caused by the use of the described service.
- The service is provided as best-effort
- MELANI/GovCERT.ch may suspend the service described herein for a specific client or for all clients at any time and without providing justification.