TLP WHITE

2022-011
23/02/2022

Banana Sulfate infrastructure cluster exposed

OBJECTIVES:
UNKNOWN

INTRUSION SET:
UNKNOWN

Summary

During their day to day threat hunting, SEKOIA.IO analysts have recently discovered an infrastructure cluster composed of 88 domain names dubbed internally “Banana Sulfate”. Despite its size and its apparent sophistication, SEKOIA.IO hasn’t any ties regarding the attribution to a particular intrusion set.

Infrastructure analysis

The majority of “Banana Sulfate” domains are resolving IP addresses hosted on **Host Sailor Ltd** (AS60117) and **MivoCloud** (AS39798) and the threat actor started to set up his infrastructure almost two years ago to the day and registered its last domain in December, 2021.

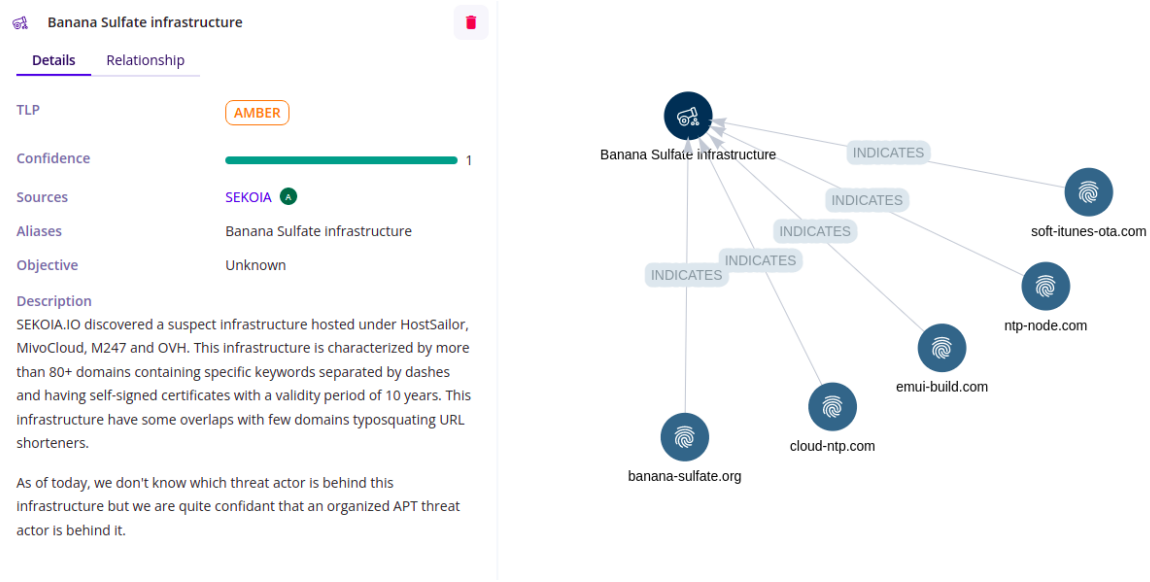

Figure 1. Banana Sulfate related domains in the SEKOIA.IO Intelligence Center

The main cluster of this infrastructure is composed of domains embedding some technical keywords separated by dashes, such as:

```
build
search
updt
socket
pkg
symcd
itunes
metrics
relay
sec
analytics
global
provider
checksum
mz
synchro
asset
smsg
node
trace
sources
diagnostic
dev
mtp
data
control
services
diag
cdnnode
soft
forward
serv
cloud
verify
online
send
updated
app
requests
emui
request
package
apt
sync
ctrl
respond
repo
ssl
layer
endpoint
updater
check
update
ntp
geomap
routing
layers
link
ota
source
smtp
ressources
tools
cts
```

It is interesting to note that one of the keywords is “emui”, which seems to refer to **Huawei EMUI**, the Huawei operating system for smartphones. Some of the VPS seen in that infrastructure are also resolving other domains which mimic **URL shorteners**, such as:

```
t2m[.]ink
cutl[.]gd
snip[.]gd
t2m[.]gd
tinurl[.]ink
budurl[.]li
biturl[.]li
lturl[.]me
```

The size of this infrastructure and the domain patterning seems to indicate that these domains are used by a well resourced APT threat actor, reminding **APT31**, **Cytrox**/**Candiru** or **NOBELIUM**. Unfortunately we haven't been able to get any URL linked to the fake url shorteners and any malicious code communicating with this infrastructure. Therefore, an attribution to a known intrusion set or activity cluster is impossible.

M1037 Filter Network Traffic - Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

IOCs & Technical Details

Domain names

```
respond-layer[.]com
symcd-itunes[.]com
nserver7-apple[.]com
cutl[.]gd
biturl[.]li
relay-analytics[.]com
cts-socket[.]com
cts-updt[.]com
lturl[.]me
urlme[.]li
tools-cts[.]com
checksum-ctrl[.]com
snip[.]gd
budurl[.]li
emui-build[.]com
pkg-updater[.]com
serv-build[.]com
updated-cloud[.]com
respond-updt[.]com
build-symcd[.]com
send-update[.]com
cloud-ntp[.]com
east-ssl-endpoint[.]com
ntp-verify[.]com
global-pkg[.]com
online-repo[.]com
repo-ssl[.]com
ntp-cts[.]com
control-updt[.]com
node-sec[.]com
```

```
ntp-node[.]com
ota-ssl[.]com
checksum-mz[.]com
soft-asset[.]com
update-ntp[.]com
app-requests[.]com
relay-apt[.]com
package-ssl[.]com
mz-provider[.]com
synchro-updt[.]com
diag-cts[.]com
link-ota[.]com
ssl-forward[.]com
diagnostic-dev[.]com
mtp-socket[.]com
t2m[.]ink
ntp-layers[.]com
cdnnode-smsg[.]com
respond-source[.]com
build-search[.]com
sync-analytics[.]com
tinurl[.]ink
mtp-sources[.]com
soft-itunes-ota[.]com
metrics-dev[.]com
routing-layers[.]com
ntp-services[.]com
request-package[.]com
updater-check[.]com
control-mtp[.]com
trace-ota[.]com
data-mtp[.]com
forward-provider[.]com
banana-sulfate[.]org
diagnostic-link[.]com
node-smsg[.]com
checksum-ota[.]com
mz-updt[.]com
source-app02[.]com
synchro-ntp[.]com
smsg-updater[.]com
repo-sec[.]com
smtp-ressources[.]com
asset-updater[.]com
ota-relay[.]com
provider-ota[.]com
check-sync[.]com
respond-layers[.]com
forward-cts[.]com
ntp-checksum[.]com
socket-metrics[.]com
ota-build[.]com
global-provider[.]com
analytics-ntp[.]com
checksum-cts[.]com
ctrl-respond[.]com
t2m[.]gd
geomap-apple[.]com
```

TTPs (ATT&CK)

Acquire Infrastructure: Domains (T1583.001)
Acquire Infrastructure: Virtual Private Server (T1583.003)

CONFIDENCE
HIGH

REFERENCES

- [SEKOIA.IO] Banana Sulfate on Intelligence Center

You can now access all FLINT reports and associated IOCs on our SEKOIA.IO Intelligence Center web portal.

https://app.sekoia.io

Our mailing address is:
SEKOIA
18-20 place de la Madeleine
Paris 75008
France

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.