Ongoing Roaming Mantis smishing campaign targeting France

blog.sekoia.io/ongoing-roaming-mantis-smishing-campaign-targeting-france/

18 July 2022

*This blog post on Roaming Mantis group is an extract of the "**FLINT 2022-037 – Ongoing Roaming Mantis smishing campaign targeting France**" report (SEKOIA.IO Flash Intelligence) sent to our clients on July 07, 2022.*

Summary

On July 4, 2022, a SEKOIA.IO analyst received phishing SMS (also called *smishing*) embedding a malicious URL. The URL either deploys the MoqHao Android malware, or redirects to an Apple login details credential harvesting page. Analysing this smishing activity led us to identify an active campaign targeting France wide victims.

Observed *modus operandi* during the ongoing campaign targeting French mobile phone users is congruent with past observed **Roaming Mantis**' activities documented by multiple security vendors. The campaigns distributing MoqHao in Japan, South Korea, Taiwan, Germany, France, the UK and the US, have similar techniques. Our investigation shows that **this campaign widely impacts France** and possibly results in around 70.000 Android device compromises.

MoqHao (aka Wroba, XLoader for Android) is an Android Remote Access Trojan (RAT) with information-stealing and backdoor capabilities that likely spreads via SMS. It is attributed to Roaming Mantis, assessed to be a financially motivated Chinese threat group.

SEKOIA.IO analysts monitor and track this threat since the beginning of 2022. In this blog post, we describe each step of the ongoing smishing campaign and share our investigation on Roaming Mantis' infrastructure.

Ongoing smishing campaign

The Roaming Mantis smishing campaign was first observed by SEKOIA.IO analysts through four malicious SMS received on two mobile phones. The distribution campaign shows geofencing and operating system checking capabilities. We assess that these features allow Roaming Mantis to tailor their attack, as well as hinder analysis and detection efforts.

Here is an overview of the infection chain depending on the victim's location (based on their IP address) and operating system (based on its user-agent).

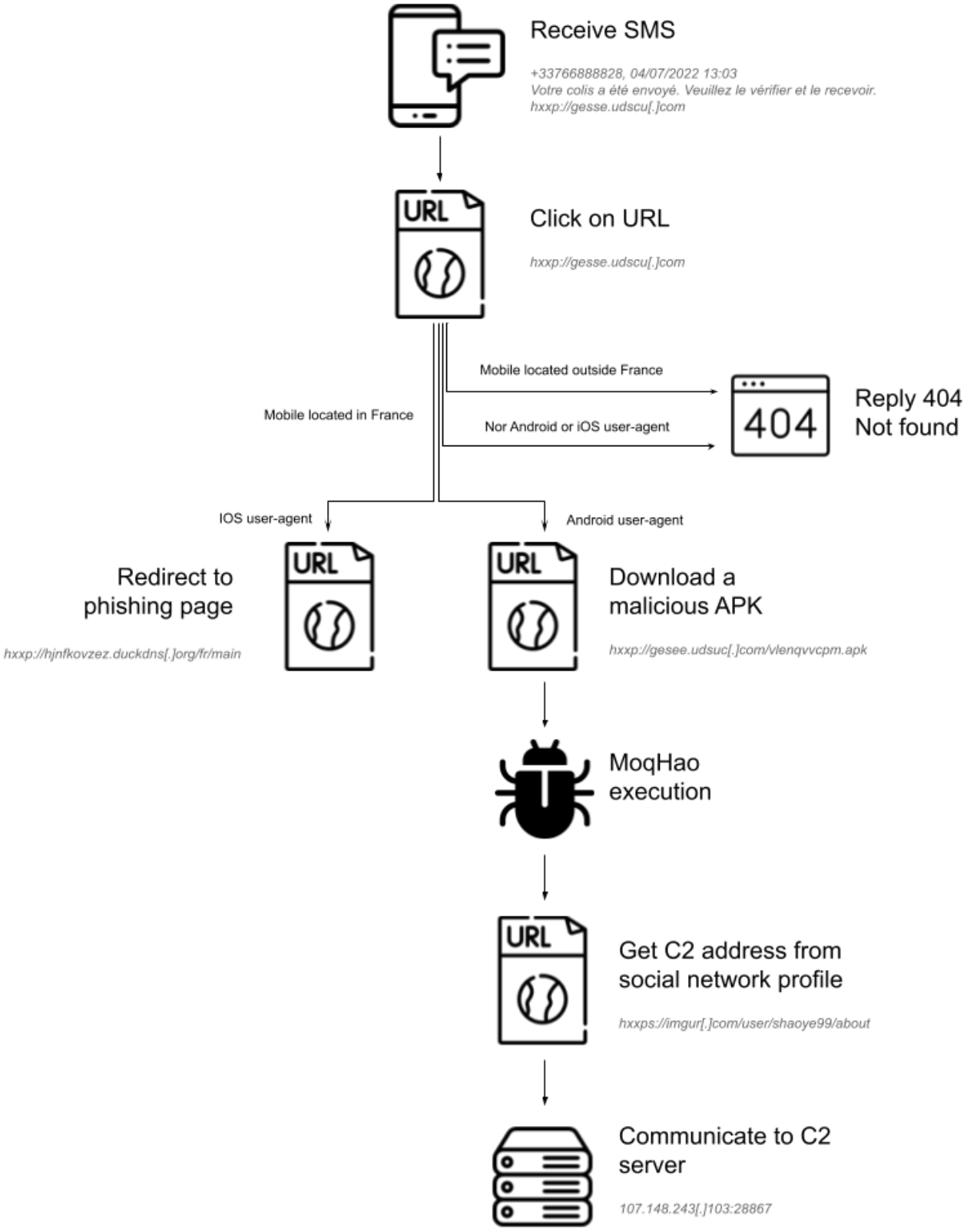

Figure 1. MoqHao's infection chain

Step-by-step MoqHao's compromise

The initial attack vector is a text message distributed by SMS and containing a malicious URL, as shown in the following figure.

Figure 2. Phishing SMS (translated from French: "Your package has been sent. Please check it and receive it.")

If the target clicks on the link, an HTTP request is sent to the server. Depending on the location of the victim (likely inferred from its IP address), and its operating system (inferred from the user-agent), the server responds:

- Nothing (404 Not found), if the victim's device is not located in France;
- An HTML page containing JavaScript code displaying an alert and redirecting to an APK (Android Package Kit) file, if the mobile is located in France and runs Android;
- A fake Apple login web page, if the mobile is located in France and is an iPhone.

The *smishing* campaign is therefore geofenced and aims to install Android malware, or collect Apple iCloud credentials.

If the victim's mobile phone is running the Android operating system, a message entices the victim to download the malicious APK as a web browser update (SHA256: 3ba2b1c0352ea9988edeb608abf2c0 37b1f30482bbc05c3ae79265bab7a44c9). This file corresponds to the MoqHao malware according to the analysis of the Hatching Triage sandbox.

Once the victim downloaded and executed the malware, the application requests permission to read and send SMS messages. This permission allows the malware, among other things, to intercept SMS from victims' mobile phones. It is worth noting the studied MoqHao sample mimics the Chrome application to lure the victim to give the permission.

The malware then retrieves its C2 server by requesting one of the social network profiles stored in the payload. In the analysed sample, the profiles are: shaoye77, shaoye88 and shaoye99 on Imgur service. In the above Triage analysis, the malware requests the profile shaoye99 on the legitimate image hosting service Imgur (hxxps://imgur[.]com/user/shaoye99/about).

As shown in the figure, the “about” section contains the string “bgfrewiFaRPCdEp9o0GfWPL3dhKU2 uwZh-Z7eg9bgfrewi” which embeds the DES-encrypted C2 server contained between the markers “bgfrewi”. By using the following recipe in CyberChef, we obtain the final IP address and port pair (107.148.243[.]103:28867).

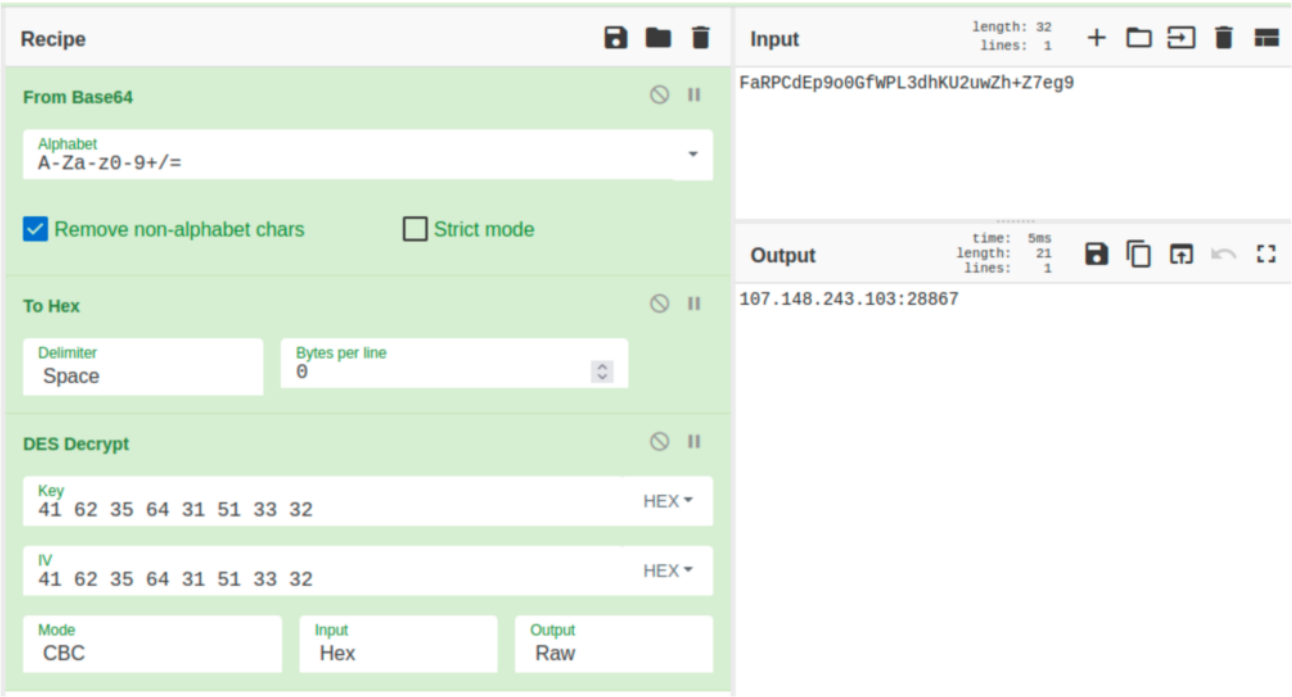

Figure 4. CyberChef recipe to decrypt the string containing the C2 server

It is worth noting the character “-” is replaced by “+” in URL safe Base64 encoding representation. Since 2020, the DES key and IV (41 62 35 64 31 51 33 32) are unchanged.

Analysis of the Roaming Mantis campaign

Chinese intrusion set Roaming Mantis is assessed to be a financially motivated group, with a history of targeting developed countries.

In addition to the received message, several French people are currently reporting this campaign on Twitter, as well as on French websites dedicated to phishing. As reported by Kaspersky and Team Cymru in early 2022, and based on our observation of **more than**

90.000 unique IP addresses that requested the C2 server distributing MoqHao, we confirm that the threat group Roaming Mantis currently focuses on France.

This activity leveraging MoqHao or Apple IDs' credential harvesting pages notably provides Roaming Mantis access to data from the local system, SD card, applications, messages or contact list, iCloud backups, iMessage, call history, as well as allowing remote interaction with a victims' device.

We assess Roaming Mantis' **wide collection of sensitive data** could be further used in extortion schemes, sold to other threat groups or possibly leveraged in "Big Game Hunting" operations.

Roaming Mantis infrastructure

We noticed two different infection chains depending on the user-agent of the target. In the following sections, we describe the infrastructure associated with these attack chains.

Android payloads

The infrastructure hosting Android payloads was detailed by Team Cymru in their part 2 blogpost from April 2022. According to our analysis, this infrastructure still has the same characteristics:

- Servers are used to target only one country, meaning if an IP address from another country contacts the servers, it will get a 404 error.
- The open ports on the servers are still the same: TCP/443,TCP/5985,TCP/10081andTCP/47001.
- The certificate identified in April is still in use on these servers:
  - SHA1: 834024f91f67445a7fd1a98689cb3f49b4c3ade7
  - SHA256: 76de629b3e446e99d45541e95da0bfa18db43a48daa23f5551fdbde0c295a36c

Apple phishing

SEKOIA analysts also studied the infrastructure of Apple phishing pages:

- Those servers have the following ports open: TCP/80, TCP/5432, TCP/5985 and TCP/47001.
- The landing page mimics the Apple ID login page. As the Android infrastructure, the geofencing is set and the landing page language matches the language of targeted users.

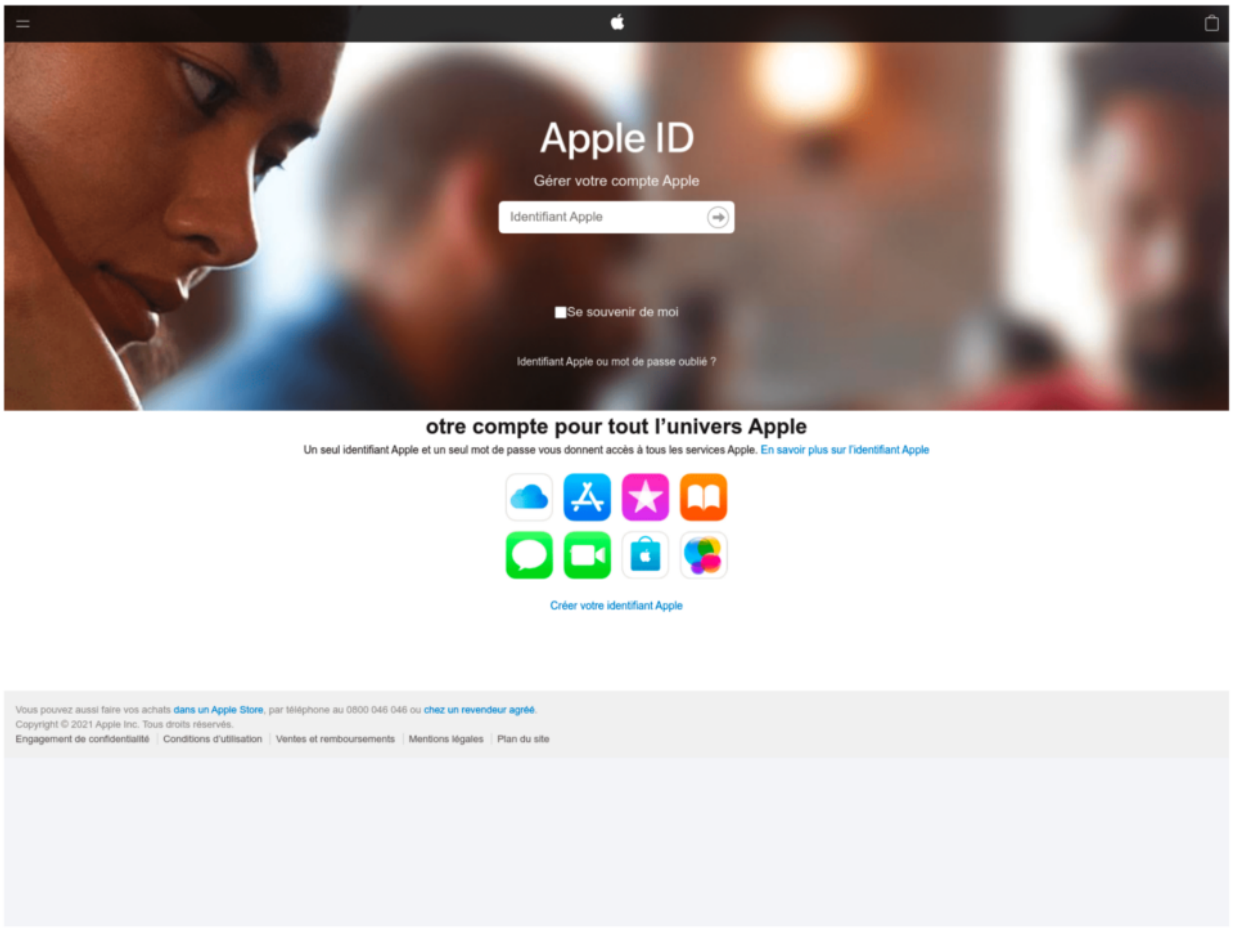

Figure 5. Apple ID phishing page in French (source: urlscan)

Those pages can be tracked on scanning services like urlscan using hashes of sub-ressources requested by the main page such as Card.js file (6d5516bbbebba2d51878f1e791b642f3b2944270b8e 84770f15a16376b202213).

Domains

Domains used inside SMS messages are either registered with Godaddy or use dynamic dns services such as duckdns.org. The intrusion set uses more than hundreds subdomains. Indeed each IP address is resolved by dozens of FQDN (eg: more than 5000 FQDN resolve to 134[.]119[.]205[.]21). As it is complex to list all domains, SEKOIA rather tracks associated IP addresses to monitor this intrusion set.

MoqHao C2 server

Roaming Mantis uses a separate infrastructure for the MoqHao C2 servers.

At the time of writing, we were able to identify 9 servers hosted on EHOSTIDC and VELIANET Autonomous Systems.

All infrastructures are monitored by SEKOIA internal project “SEKOIA C2 Trackers” and can be found in our Intelligence Center portal.

Discover our CTI and XDR products

MITRE ATT&CK TTPs

T1583.001 – Acquire Infrastructure: Domains
T1583.004 – Acquire Infrastructure: Server
T1583.006 – Acquire Infrastructure: Web Services
T1566.002 – Phishing: Spearphishing Link
T1204.001 – User Execution: Malicious Link
T1102.001 – Web Service: Dead Drop Resolver
T1071.001 – Application Layer Protocol: Web Protocols
T1041 – Exfiltration Over C2 Channel

MoqHao malware IOCs & Technical Details

Domains contained in SMS

```
coqrf.xpddg[.]com
znjjq.udsuc[.]com
gesee.udsuc[.]com
bswhd.mrheu[.]com
xpddg[.]com
udsuc[.]com
mrheu[.]com
```

Malicious APK

```
83ba2b1c0352ea9988edeb608abf2c037b1f30482bbc05c3ae79265bab7a44c9
```

APK permissions

```
android.permission.BROADCAST_SMS
android.permission.BROADCAST_WAP_PUSH
android.permission.SEND_RESPOND_VIA_MESSAGE
android.permission.ACCESS_WIFI_STATE
android.permission.BROADCAST_WAP_PUSH
android.permission.SEND_RESPOND_VIA_MESSAGE
android.permission.ACCESS_WIFI_STATE
android.permission.CHANGE_NETWORK_STATE
android.permission.CALL_PHONE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.READ_EXTERNAL_STORAGE
android.permission.ACCESS_NETWORK_STATE
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.WAKE_LOCK
android.permission.INTERNET
android.permission.RECEIVE_SMS
android.permission.READ_SMS
android.permission.WRITE_SMS
android.permission.SEND_SMS
android.permission.SYSTEM_ALERT_WINDOW
android.permission.READ_CONTACTS
android.permission.READ_PHONE_STATE
android.permission.GET_ACCOUNTS
```

Android payload servers

```
134[.]119[.]193[.]106
134[.]119[.]193[.]108
134[.]119[.]193[.]109
134[.]119[.]193[.]110
134[.]119[.]205[.]18
134[.]119[.]205[.]21
134[.]119[.]205[.]22
142[.]0[.]136[.]49
142[.]0[.]136[.]50
142[.]0[.]136[.]52
142[.]4[.]97[.]105
142[.]4[.]97[.]106
142[.]4[.]97[.]107
142[.]4[.]97[.]108
142[.]4[.]97[.]109
146[.]0[.]74[.]157
```

146[.]0[.]74[.]197
146[.]0[.]74[.]199
146[.]0[.]74[.]202
146[.]0[.]74[.]203
146[.]0[.]74[.]205
146[.]0[.]74[.]206
146[.]0[.]74[.]228
192[.]51[.]188[.]107
192[.]51[.]188[.]108
192[.]51[.]188[.]109
192[.]51[.]188[.]142
192[.]51[.]188[.]145
192[.]51[.]188[.]146
27[.]124[.]36[.]32
27[.]124[.]36[.]34
27[.]124[.]36[.]52

27[.]124[.]39[.]241
27[.]124[.]39[.]242
27[.]124[.]39[.]243
91[.]204[.]227[.]19
91[.]204[.]227[.]20
91[.]204[.]227[.]21
91[.]204[.]227[.]22
91[.]204[.]227[.]23
91[.]204[.]227[.]24
91[.]204[.]227[.]25
91[.]204[.]227[.]26
91[.]204[.]227[.]27
91[.]204[.]227[.]28

Apple phishing servers

172[.]81[.]131[.]12
172[.]81[.]131[.]14
172[.]81[.]131[.]10
172[.]81[.]131[.]11
172[.]81[.]131[.]13
103[.]80[.]134[.]41
103[.]80[.]134[.]40
103[.]80[.]134[.]42

MoqHao C2 servers

```
61[.]97[.]248[.]6
61[.]97[.]248[.]7
61[.]97[.]248[.]8
61[.]97[.]248[.]9
103[.]249[.]28[.]206
103[.]249[.]28[.]207
103[.]249[.]28[.]208
103[.]249[.]28[.]209
92[.]204[.]255[.]172
```

Imgur profile used as Dead Drop resolvers

```
hxxps://imgur[.]com/user/shaoye99/about
hxxps://imgur[.]com/user/shaoye88/about
hxxps://imgur[.]com/user/shaoye77/about
hxxps://imgur[.]com/user/shaoye66/about
hxxps://imgur[.]com/user/shaoye55/about
hxxps://imgur[.]com/user/shaoye44/about
hxxps://imgur[.]com/user/shaoye33/about
hxxps://imgur[.]com/user/shaoye22/about
hxxps://imgur[.]com/user/shaoye11/about
```

IoCs are available on the SEKOIA.IO Community Github: https://github.com/SEKOIA-IO/Community/blob/main/IOCs/roamingmantis/roaming_mantis_iocs_20220718.csv

More IoCs related to MoqHao malware or Roaming Mantis intrusion set are available on SEKOIA.IO for our XDR and CTI customers.

Chat with our team!

Would you like to know more about our solutions? Do you want to discover our XDR and CTI products? Do you have a cybersecurity project in your organization? Make an appointment and meet us!

Contact us
You can find out how we track threats on our SOC platform SEKOIA.IO.