MoqHao Part 3: Recent Global Targeting Trends

team-cymru.com/post/moqhao-part-3-recent-global-targeting-trends

S2 Research Team March 16, 2023

Introduction

This blog post is part of an ongoing series of analysis on MoqHao (also referred to as Wroba and XLoader), a malware family commonly associated with Roaming Mantis. MoqHao is generally used to target Android users, often via an initial attack vector of phishing SMS messages (smishing).

The threat group behind Roaming Mantis are characterized as Chinese-speaking and financially motivated, first public acknowledgement goes back to around 2018. The group has historically targeted countries in the Far East – Japan, South Korea and Taiwan, but they are expanding their campaign.

In our most recent post (MoqHao Part 2: Continued European Expansion), we demonstrated how Roaming Mantis had widened their sights to Western countries, including France, Germany, the United Kingdom, and the United States.

Further Reading

- MoqHao Part 1.5: High-Level Trends of Recent Campaigns Targeting Japan
- MoqHao Part 1: Identifying Phishing Infrastructure

In this post we will explore whether Roaming Mantis have continued to expand their operations over the past year, focusing on their activities in recent months. In doing so we will seek to highlight some techniques which we have utilized to pivot to connected infrastructure.

Key Findings

- Identification of 14 MoqHao C2 servers, based on malware analysis and pivots within contextual data sets.
- Evidence of Roaming Mantis campaigns targeting every continent, with Africa, Asia, and Europe the most impacted.
- Close to 1.5 million victim communications to the MoqHao C2 servers observed since the end of 2022.
- The scope of Roaming Mantis continues to grow; all mobile users should be conscious of smishing threats, particularly from operators who have evolved their campaigns over several years.

MoqHao Command & Control

As in previous posts, our analysis begins with the identification of infrastructure utilized for the purpose of post-infection communications, once a malicious APK (MoqHao) has been installed on a victim device.

The rationale for this approach is two-fold:

1. The delivery and installation methodology for MoqHao includes the use of ‘disposable’ staging infrastructure which generally utilizes Dynamic DNS services, in addition to legitimate platforms, such as Baidu, Imgur, Pinterest, and VKontakte. Analysis of network telemetry data associated with these phases of an infection is complicated by the presence of security research, scanning, and (large volume) benign user activity. Furthermore, until beacons to a Moqhao C2 server are observed, it is not wholly accurate to identify any communications as ‘victim’ related.
2. Whilst MoqHao’s delivery infrastructure has a short shelf life, its C2 infrastructure is used for extended periods of time and in some cases even reused after periods of inactivity. By analyzing stable infrastructure, we can draw higher level conclusions on targeting, i.e., where large groupings of victim connections originate from. In addition, as this infrastructure is more static, by disclosing it we can have the greatest impact on Roaming Mantis operations.

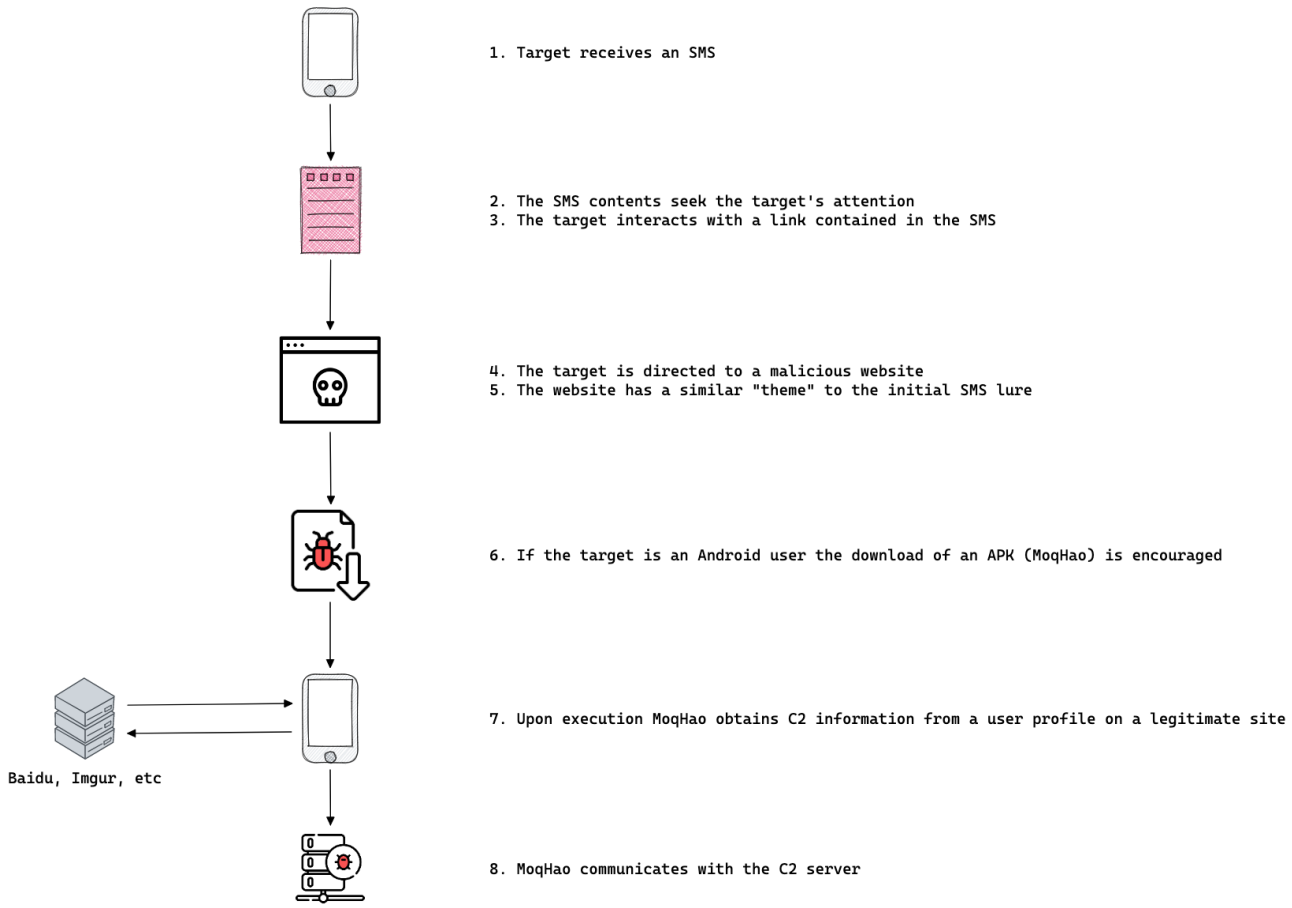

Figure 1: Simplified Delivery Chain for MoqHao

Our initial method of identifying MoqHao C2 infrastructure is based on analysis of malware samples. In this case we have started with three malware samples identified within our internal malware holdings, which are also available in VirusTotal.

MoqHao is detected by several antivirus vendors as 'Wroba', querying for this string within malware repositories will generally lead to connected samples.

37134b50f0c747fb238db633e7a782d9832ae84b

---

*This file was first uploaded on 24 October 2022 by a user in Canada, it is configured to receive C2 information (**91.204.227.31**:28877) from a user profile on VKontakte.*

Examining network telemetry for **91.204.227.31** (HDTIDC - South Korea) we observe a campaign targeting users in Australia, with the most recent victim connections occurring around 29 January 2023.

Open Ports information for **91.204.227.31** identifies that TCP/5985 was open during the period when victim connections occurred. The banner data obtained from scanning that port contains reference to a Computer / Domain Name - **WIN-VLVN3FLKKGL**.

```
WinRM NTLM Info:
  OS: Windows 10/Windows Server 2019
  OS Build: 10.0.17763
  Target Name: WIN-VLVN3FLKKGL
  NetBIOS Domain Name: WIN-VLVN3FLKKGL
  NetBIOS Computer Name: WIN-VLVN3FLKKGL
  DNS Domain Name: WIN-VLVN3FLKKGL
  FQDN: WIN-VLVN3FLKKGL
```

Figure 2: Open Ports Information for 91.204.227.31

Pivoting on the **WIN-VLVN3FLKKGL** value we identified four additional IP addresses, all within 91.204.227.0/26.

We found victim communications to three of these IP addresses, two of which were identified in previous reporting (by Kaspersky) as MoqHao C2 servers:

- **91.204.227.32 << Kaspersky C2**
- **91.204.227.33 << Kaspersky C2**
- **91.204.227.51**

The first two C2s are used in campaigns primarily targeting users located in Asia, but also Australia (as was the case with **91.204.227.31**). A significant proportion of victims were in Japan, Nepal, and Thailand.

91.204.227.51 was used as the C2 server for a campaign targeting users in France, with the last victim connections observed around 26 February 2023.

198b55d4e7c7c0ee4fc4cbe13859533e651b91f6

This file was first uploaded on 20 February 2023 by a user in Canada, it is configured to receive C2 information (**198.144.149.142**:28866) from a user profile on VKontakte.

Examining network telemetry for **198.144.149.142** (NETMINDERS - Canada) we observe a campaign targeting users globally - in Africa, Asia, Europe, North America, and Oceania, with victim connections still occuring at the time of writing.

Open Ports information for **198.144.149.142** identifies an RDP certificate hosted on TCP/3389 with a Common Name value of **sid380**.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 532009237934085435599383654541270678 78 (0x2806200e6faa9fb24d3cf87e6379f2e6)
    Signature Algorithm: SHA256-RSA
        Issuer: CN=sid380
        Validity
            Not Before: Feb 8 21:01:38 2023 UTC
            Not After : Aug 10 21:01:38 2023 UTC
        Subject: CN=sid380
        Subject Public Key Info:
            Public Key Algorithm: RSA
                Public-Key: (2048 bit)
                Modulus:
                    ab:af:45:cf:77:6b:9f:cf:dd:bc:a2:3a:7b:70:15:
                    46:7f:78:44:45:53:a0:02:9e:9f:19:81:e0:81:aa:
                    b4:4e:f5:f0:86:c2:61:05:44:a7:80:ac:f0:80:9d:
                    e3:62:78:a7:4c:e0:f5:39:b8:77:7f:8e:74:37:b5:
                    d8:d9:76:18:7a:31:db:0a:48:06:fe:e7:63:63:2d:
                    15:cd:24:9b:d2:e0:4e:66:db:2d:96:3c:15:93:8a:
                    c3:03:81:95:ef:45:70:37:b3:d6:21:25:16:5d:4a:
                    b4:5d:19:32:17:e8:96:7b:b7:f9:be:08:42:f4:19:
                    f1:10:1c:26:95:33:76:69:96:42:fa:dc:50:10:91:
                    0d:c4:8c:70:40:33:80:29:da:da:9e:f8:b3:45:f3:
                    47:3b:33:2d:69:26:d0:32:c5:52:46:da:52:48:df:
                    86:72:63:9c:e0:98:d6:ea:d8:f5:02:f8:86:71:e9:
                    59:62:9c:a9:b7:b8:19:ee:42:e6:90:fc:c0:ed:97:
                    bf:40:d7:bd:f3:f4:33:98:90:26:68:48:a1:77:a1:
                    00:2f:e5:dd:d5:39:90:4b:eb:51:78:9a:86:13:62:
                    a3:d6:a3:aa:ef:76:44:55:6d:7a:70:51:c2:b5:08:
                    cc:5a:52:35:cd:dc:65:cd:68:f8:03:13:72:92:d9:
                    3d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
```

Figure 3: Certificate Data for 198.144.149.142

Pivoting on the **sid380** value we identified 12 additional IP addresses, all within 198.144.149.128/28.

We found victim communications to one of these IP addresses, which was identified in the Kaspersky reporting as a MoqHao C2 server:

198.144.149.131 << Kaspersky C2

As in the case of **198.144.149.142**, this C2 is used in campaigns targeting users globally, further including South America (Brazil and Suriname).

5ceb8950759a8d9d31389d1370d381d158c79fbe

This file was first uploaded on 25 February 2023 by a user in Japan, it is configured to receive C2 information (**91.204.227.43**:29872) from a user profile on VKontakte.

Examining network telemetry for **91.204.227.43** (HDTIDC - South Korea) we observe a campaign targeting users in India, with the most recent victim connections occurring around 03 March 2023.

Open Ports information for **91.204.227.43** identifies that TCP/5985 was open during the period when victim connections occurred. The banner data obtained from scanning that port contains reference to a Computer / Domain Name - **M172-17-64-184**.

```
WinRM NTLM Info:
  OS: Windows 10/Windows Server 2019
  OS Build: 10.0.17763
  Target Name: M172-17-64-184
  NetBIOS Domain Name: M172-17-64-184
  NetBIOS Computer Name: M172-17-64-184
  DNS Domain Name: m172-17-64-184
  FQDN: m172-17-64-184
```

Figure 4: Open Ports Information for 91.204.227.43

Pivoting on the **M172-17-64-184** value we identified 13 additional IP addresses, all within 91.204.227.0/26.

We found victim communications to seven of these IP addresses, one of which was identified in the Kaspersky reporting as a MoqHao C2 server:

91.204.227.37

Campaigns targeting users in Turkey and the United States.

91.204.227.39 << Kaspersky C2

Campaigns primarily targeting users in India and Nepal, with additional targeting in the Middle East and North America.

91.204.227.41

A campaign targeting users in South Africa.

91.204.227.42

Campaigns primarily targeting users in Europe (Austria and Czech Republic), with additional targeting in Asia and the Middle East.

91.204.227.47

Campaigns targeting users in Malaysia and Nepal.

91.204.227.48

A campaign targeting users in the Czech Republic, with additional targeting in Belgium, the Dominican Republic, and Turkey.

91.204.227.49

Campaigns targeting users in India, Portugal, South Africa, and the United Kingdom, with smaller clusters of victims globally (Africa, Asia, Europe, the Middle East, North America, and Oceania).

Conclusion

Whilst this analysis is caveated by the fact it is based on sampled data, and that some researcher / scanning activity likely slipped through our net, we were able to identify connections, indicative of victims, from 67 distinct countries.

Approximately 80% of connections were from the East Asian region (primarily Japan), which could be referred to as the ‘traditional’ operating base of Roaming Mantis. However, when you remove those connections from the data, you’re left with a picture of the operators’ efforts to expand globally.

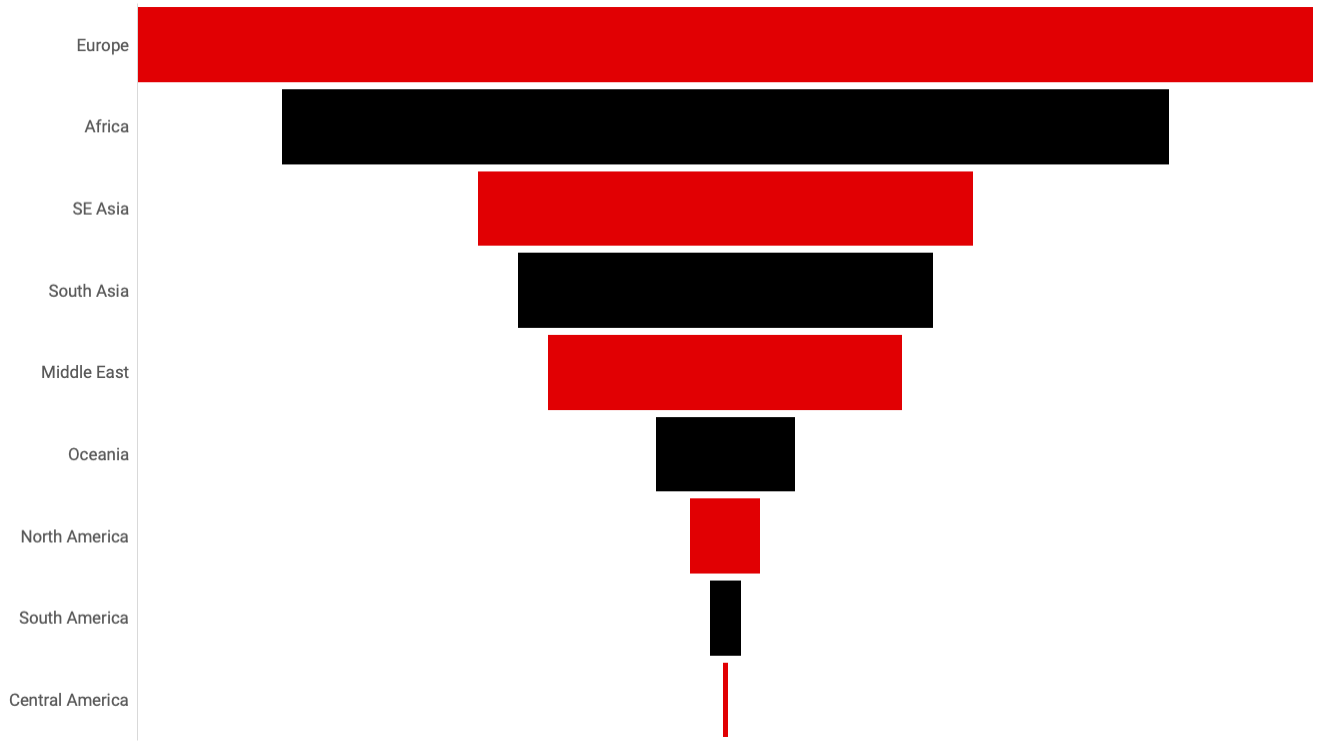

Figure 5: Spread of Victim Communications

Users from Africa, other regions in Asia, and Europe in particular are increasingly appearing in victim communications to MoqHao infrastructure.

Smishing often doesn't receive the same level of attention as phishing when it comes to the malware delivery stakes. But, with over 1 million observed victim connections since the end of 2022 related to Roaming Mantis alone, it is clearly a viable initial access vector.

If Roaming Mantis can develop their delivery methods globally, to match the depth and 'real feel' spoofing of their East Asian campaigns, we would anticipate that the threat to users will continue to grow over coming months and years.

Recommendations

- We encourage continued education on mobile device security in general and smishing more specifically, to arm users with the knowledge required to identify and avoid threats.
- Where feasible, connections to the static MoqHao C2 servers listed in the IOC section below should be pre-emptively blocked.
- Users of Pure Signal Recon can track MoqHao campaigns based on the methods described in this blog post.

IOCs

MoqHao Samples

198b55d4e7c7c0ee4fc4cbe13859533e651b91f6

37134b50f0c747fb238db633e7a782d9832ae84b

5ceb8950759a8d9d31389d1370d381d158c79fbe

MoqHao C2 Servers (With Port Pairings 🍷)

ACTIVE (14 March 2023)

HDTIDC LIMITED - South Korea:

91.204.227.32:28877

91.204.227.33:28899

91.204.227.37:28836

91.204.227.37:28856

91.204.227.39:28844

91.204.227.41:29869

91.204.227.42:29871

91.204.227.47:28999

91.204.227.48:28843

91.204.227.49:29870

NETMINDERS - Canada:

198.144.149.131:28866

198.144.149.142:28866

INACTIVE (Date)

HDTIDC LIMITED - South Korea:

91.204.227.31:28877 (29 January 2023)

91.204.227.43:29872 (03 March 2023)

91.204.227.51:36599 (26 February 2023)

NETMINDERS - Canada:

198.144.149.131:28867 (05 January 2023)

198.144.149.131:28868 (22 February 2023)

198.144.149.131:28869 (03 January 2023)