MoqHao Part 2: Continued European Expansion

team-cymru.com/blog/2022/04/07/moqhao-part-2-continued-european-expansion/

S2 Research Team View all posts by S2 Research Team April 7, 2022

This blog is a product of ongoing collaboration with @ninoseki, a Tokyo-based researcher who has tracked MoqHao for several years. His public GitHub contains numerous useful OSINT threat hunting tools.

Introduction

MoqHao (also referred to as Wroba and XLoader) is a malware family commonly associated with the Roaming Mantis threat actor group. MoqHao is generally used to target Android users, often via an initial attack vector of phishing SMS messages (smishing).

Roaming Mantis are characterized as Chinese-speaking and financially motivated. The group has historically targeted countries in the Far East – in particular Japan, South Korea and Taiwan.

We have previously blogged on a MoqHao campaign targeting Japan during the Golden Week holiday period in April/May 2021.

In the recent past, several vendors (e.g., Kaspersky) have noted an expansion in Roaming Mantis' operations to include several European countries.

.

Figure 1: Tweet by @ninoseki highlighting MoqHao campaigns targeting France and Germany (August 2021)

In this blog we will examine open-source hints attributable to the threat actors, coupled with Team Cymru's insights, to provide an assessment of Roaming Mantis' current target base.

Landing Pages

When following a malicious link distributed in a Roaming Mantis smishing campaign, users are directed to a landing page. These pages are tailored specifically to a target country / language; users from other regions are presented with an error page (404 – resource not found).

Based on the user-agent information for the connecting device, one of two outcomes will occur:

.

- For Android devices, a malicious APK (MoqHao) is downloaded.
  .
- For Apple (iOS) devices, the user is presented with a phishing page where they are asked to enter credentials for a spoofed entity.

Landing Page Characteristics

To determine common characteristics of the infrastructure utilized for the hosting of Roaming Mantis landing pages, 43 IP addresses, which were observed hosting these pages since the beginning 2022, were analyzed. The following findings were true across all the IPs:

.

- The re-use of the same X.509 certificate (SHA1: 834024f91f67445a7fd1a98689cb3f49b4c3ade7), hosted on TCP/443. This certificate has a *common name* value of localhost and an *alt name* value which contains (at the time of reporting) 335 legitimate domains, summarized as follows:
  - South Korean entities, such as Naver and Daum.
  - ccTLDs for .kr (South Korea) and .tw (Taiwan).
    .
- The presence of Merlin command and control (C2) infrastructure listening on TCP/443, based on the detection of a JARM fingerprint for this service (29d21b20d29d29d21c41d21b21b41d494e0df9532e75299f15ba73156cee38).
  .
- Open ports; TCP/5985, TCP/10081, TCP/47001.
  .

Passive scanning of TCP/10081 on the landing page hosting IPs indicated an additional HTTP service listening on this port. The *HTML title* value for this service provides useful insight into victim targeting, as summarized in Table 1 below.

Landing IP	WHOIS	HTML Title	Translation
142.0.136.49	PEGTECHINC, US	美国下载	US Download
142.0.136.50			
142.0.136.52			
142.4.97.105			
142.4.97.106			

Landing IP	WHOIS	HTML Title	Translation
142.4.97.107			
142.4.97.108			
142.4.97.109			
134.119.193.106	VELIANET-AS, DE	英国下载	UK Download
134.119.193.108			
134.119.193.109			
134.119.193.110			
192.51.188.142	HDTIDC LIMITED, HK		
192.51.188.145			
192.51.188.146			
27.124.36.25	BGPNET Global ASN, SG	韩国下载	South Korea Download
27.124.36.27			
27.124.36.32			
27.124.36.52			
27.124.39.241			
27.124.39.242			
27.124.39.243			
192.51.188.101	HDTIDC LIMITED, HK	日本下载	Japan Download
192.51.188.103			
192.51.188.111			
192.51.188.14			
91.204.227.111			
91.204.227.15			
91.204.227.18			
91.204.227.20			

Landing IP	WHOIS	HTML Title	Translation
91.204.227.30			
91.204.227.32			
91.204.227.40			
146.0.74.157	HOSTKEY-AS, NL	德国下载	Germany Download
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			
134.119.205.21	VELIANET-AS, DE	法国下载	France Download
134.119.205.22			

Table 1: Insight derived from TCP/10081 on the Landing Page hosting IPs

As can be seen, in addition to campaigns targeting France, Germany, Japan, South Korea, and the United States, infrastructure was set up for the specific targeting of UK-based users. This finding would indicate a further expansion of Roaming Mantis' operations within Europe.

MoqHao Command & Control

In this section we will examine network telemetry relating to the connections made once the malicious APK (MoqHao) is installed on a victim Android device.

By examining this stage of the attack, it is possible to identify potential victims with a higher degree of certainty. This confidence is based on the chain of events leading to this point, i.e., a user has interacted with a link contained within an SMS message, visited a landing page, and the malicious APK has successfully been deployed on the user's device to the point where it has begun to beacon to the C2 server.

The starting point for this part of the analysis was a MoqHao sample (SHA1: 74558f86e4b4513f7f52d6b99b7e06d978aec97b) uploaded to VirusTotal by a user in the United Kingdom on March 16, 2022.

Analysis of this sample identified a C2 server hosted on 103.249.28.207 (EHOSTICT, KR). Network telemetry for this IP revealed a small number of connections inbound on TCP/28866, sourced from IP addresses assigned to UK mobile providers.

In addition, 103.249.28.207 was observed as a C2 server in what appeared to be four further campaigns:

.

- TCP/28866 – Spain, Turkey

  .
- TCP/29869 – South Africa

  .
- TCP/28844 – Afghanistan, Bangladesh, India, Iran, and Pakistan (South Asia)

  .

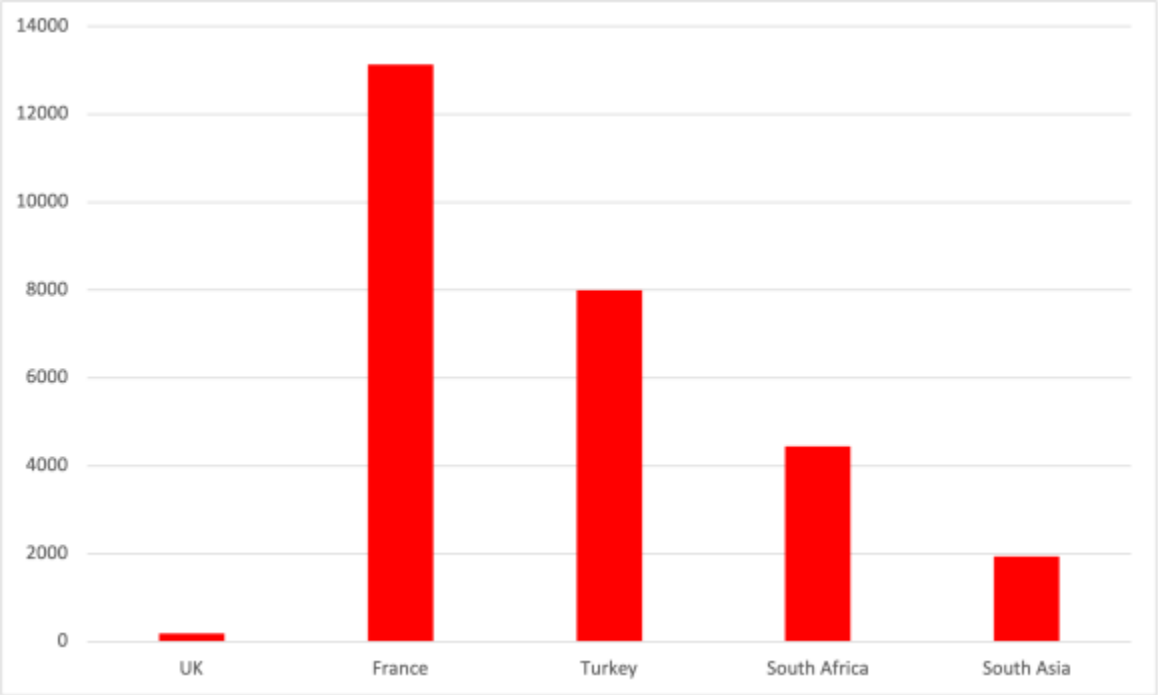

Figure 2: Victim connections to 103.249.28.207

.

Passive scanning of 103.249.28.207 identified open TCP/3389 (commonly associated with the Remote Desktop Protocol (RDP)), with a machine name of WIN-MM79JTRSTL7.

As an aside, screen captures of RDP activity on 103.249.28.207, sourced from Shodan, provided another ‘Chinese’ flag for this activity.

As recently as January 05, 2022, a remote login page was captured (associated with machine name WIN-MM79JTRSTL7), which indicated Chinese language settings – the characters 密码, meaning ‘password’ in Mandarin, were displayed.

.

Figure 3: Remote login portal for 103.249.28.207 (January 2022)

.

This login page was visible dating back to the end of 2020, all the time associated with the same machine name (WIN-MM79JTRSTL7). A screen capture from January 22, 2020, indicated Korean language settings – the characters 암호, meaning ‘password’ in Korean, were displayed.

.

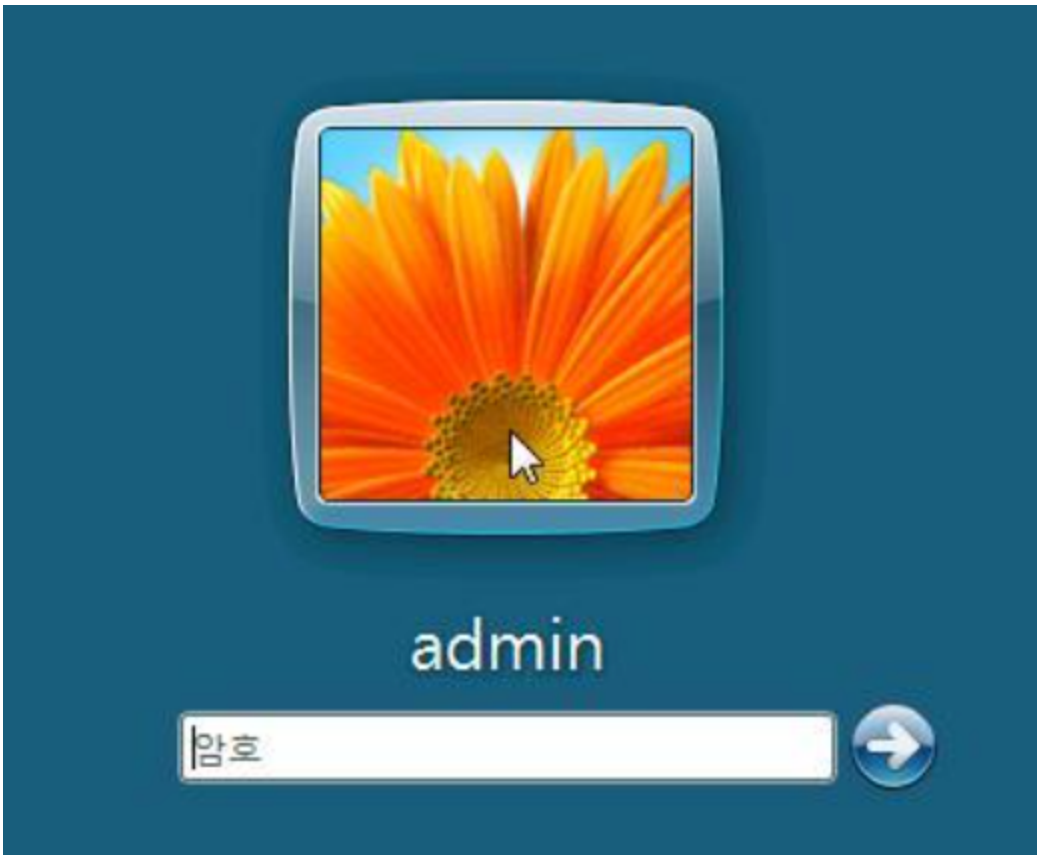

Figure 4: Remote login portal for 103.249.28.207 (January 2020)

.
Given that 103.249.28.207 is assigned to a South Korean provider (Ehost IDC), the information from Shodan may be indicative of a Chinese-speaking user accessing / utilizing the machine since late 2020.

A pivot on the value WIN-MM79JTRSTL7 identified a further eight IP addresses, all assigned to EHOSTICT, KR, which were accessed by the same machine. Network telemetry data was obtained for these IPs for the beginning of 2022 onwards, where MoqHao campaigns were identified, they are referenced in Table 2 below

IP Address	C2 Port	Target Countries
103.249.28.206	37689	China, Hong Kong, Japan, Singapore, Taiwan
103.249.28.208	38866, 38876	Taiwan
103.249.28.209	28856	United States
103.249.28.210	N/A	No active campaigns
61.97.248.5	28836	Turkey

IP Address	C2 Port	Target Countries
61.97.248.6	N/A	No active campaigns
61.97.248.7	N/A	No active campaigns
61.97.248.8	N/A	No active campaigns

Table 2: Summary of MoqHao C2 servers

.
In the case of 103.249.28.210, samples uploaded to VirusTotal in early 2021 provide an indication as to when it was an active MoqHao C2. For the remaining IPs it is not clear if they were previously MoqHao C2s. One possibility may be that they are being configured for future use.

Although not an exhaustive study of MoqHao C2 infrastructure, it is clear from the findings of this analysis and other findings from the community, that Roaming Mantis continue to expand their operations. What was previously considered to be a regional threat now has a global footprint.

Indicators of Compromise

MoqHao C2 Servers

103.249.28.206
103.249.28.207
103.249.28.208
103.249.28.209
61.97.248.5
.

MoqHao Sample

74558f86e4b4513f7f52d6b99b7e06d978aec97b