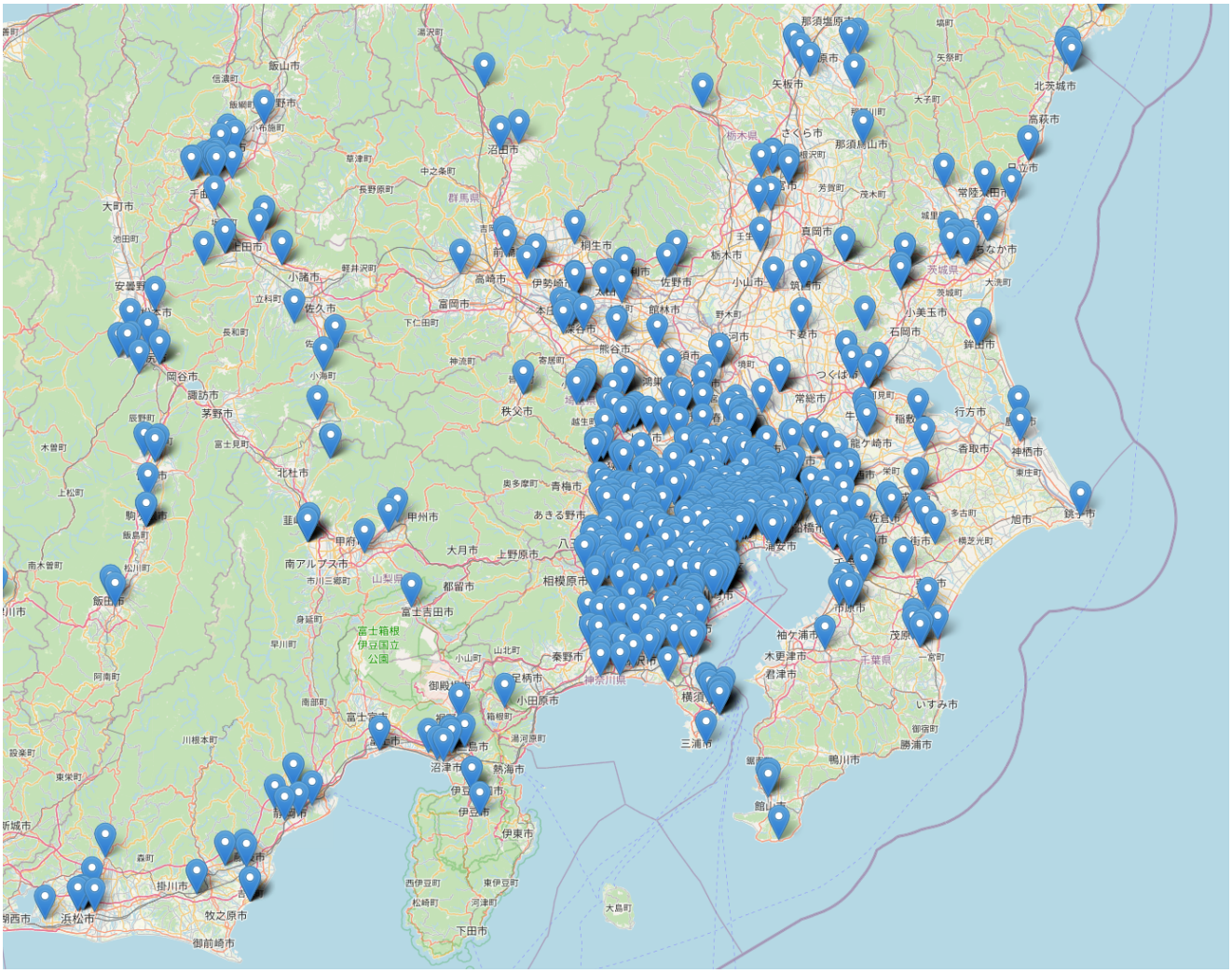
MoqHao Part 1.5: High-Level Trends of Recent Campaigns Targeting Japan

team-cymru.com/blog/2021/08/11/moqhao-part-1-5-high-level-trends-of-recent-campaigns-targeting-japan/

S2 Research Team View all posts by S2 Research Team August 11, 2021



Having last looked at the MoqHao (or Roaming Mantis) malware family in January 2021, we decided to take another look at the activities of this threat group. MoqHao targets Android users, usually via an initial attack vector of phishing SMS messages, with a particular focus on Japan, South Korea and Taiwan (although MoqHao's focus continues to expand).

Several researchers are actively tracking MoqHao's phishing infrastructure, with IOCs posted daily on forums such as Twitter. For example:

- @KesaGataMe0
- @NaomiSuzuki
- @ninoseki
- @papa_anniekey

These researchers do a great job of identifying the latest campaigns, and this blog will not seek to duplicate their findings. Instead, we will use Team Cymru's internet telemetry data to examine a subset of MoqHao campaigns, from the period April – June 2021, to provide additional insight into their scale and regularity.

This blog will be the first in a series which looks at various elements of the MoqHao infrastructure, beginning first with users targeted in Japan.

Duck DNS

MoqHao commonly uses domains generated through the dynamic DNS service Duck DNS for its first-stage delivery infrastructure. The hosting IP addresses for these domains appear to be limited to MoqHao whilst campaigns are active, shared hosting is rarely observed.

The domains utilized are generally a mix of randomly generated strings, with some spoofing of related entities. For example, amongst the domains used in this research were a number that spoofed NTT Docomo, a Japanese mobile phone operator. A regular expression can be used for matching on these domains:

[a-z]{10}.duckdns.org – e.g., docomoawbr.duckdns.org

The domain and hosting IP address pairs used in this research are shared on our public GitHub.

Network Telemetry

A set of hosting IP addresses, assigned to three providers, were used as the seeds for this analysis:

- HDTIDC Limited – South Korea
- Ophidian Network Limited – Ukraine
- Zenlayer Inc – United States

All the IP addresses were identified within Team Cymru's internal Passive DNS data sets and were observed hosting first-stage domains of the format described above. The IPs appear to be active for several days (on average around 14 days) hosting multiple domains, which update on a much more frequent basis. Therefore, blocklists based on individual domain names are not an effective countermeasure to this threat.

The table below provides a summary of the hosting IP addresses, including details on when they were first reported in open source, when victim traffic first appeared within Team Cymru's data holdings and the total number of victim connections observed.

IP Address	Whois	First Reported	Traffic First Seen	Traffic Volume
128.14.75.50	ZEN-ECN, US	03 April 2021	03 April 2021	188

103.80.134.151	HDTIDC LIMITED, KR	03 April 2021	10 April 2021	1,432
103.80.134.153	HDTIDC LIMITED, KR	03 April 2021	29 April 2021	10,024
103.80.134.171	HDTIDC LIMITED, KR	03 April 2021	15 May 2021	3,713
87.120.36.215	OPI-NET-LTD, UA	24 May 2021	25 May 2021	10,001
107.148.191.22	ZEN-ECN, US	26 May 2021	25 May 2021	622
103.80.134.177	HDTIDC LIMITED, KR	27 May 2021	26 May 2021	2,009
165.3.91.227	ZEN-ECN, US	29 May 2021	29 May 2021	61
165.3.91.228	ZEN-ECN, US	01 June 2021	31 May 2021	184
103.80.134.178	HDTIDC LIMITED, KR	05 June 2021	05 June 2021	1,389
103.80.134.180	HDTIDC LIMITED, KR	15 June 2021	15 June 2021	2,794

Table 1: MoqHao Distribution Infrastructure Summary

As can be seen, there is generally a close proximity between distribution servers becoming active (receiving victim communications) and them being reported on Twitter – usually one day or less.

HDTIDC LIMITED, KR

To account for differences in our coverage between the three providers used for first-stage domain hosting, we focused further on the six IP addresses within 103.80.134.0/24 assigned to HDTIDC Limited.

Comment: With all things being equal in terms of the (inferred) destination of the traffic analysed, we can discern more accurate patterns in the data.

Looking at inbound connections on TCP/80 sourced from IP addresses assigned to Japanese broadband/telecoms providers, we can see a daily average of around 200-300 potential victim connections to the distribution servers. On 29 April a spike in activity was noted, lasting for around 10 days – coinciding with the beginning of the Golden Week holiday period in Japan.

It is possible that the actors behind MoqHao increased their phishing activities to coincide with this period and thus generated more victims.

The figure below shows daily connections to the distribution IP addresses in combination with when each of these was seen active (outside of these periods of activity there were zero connections observed).

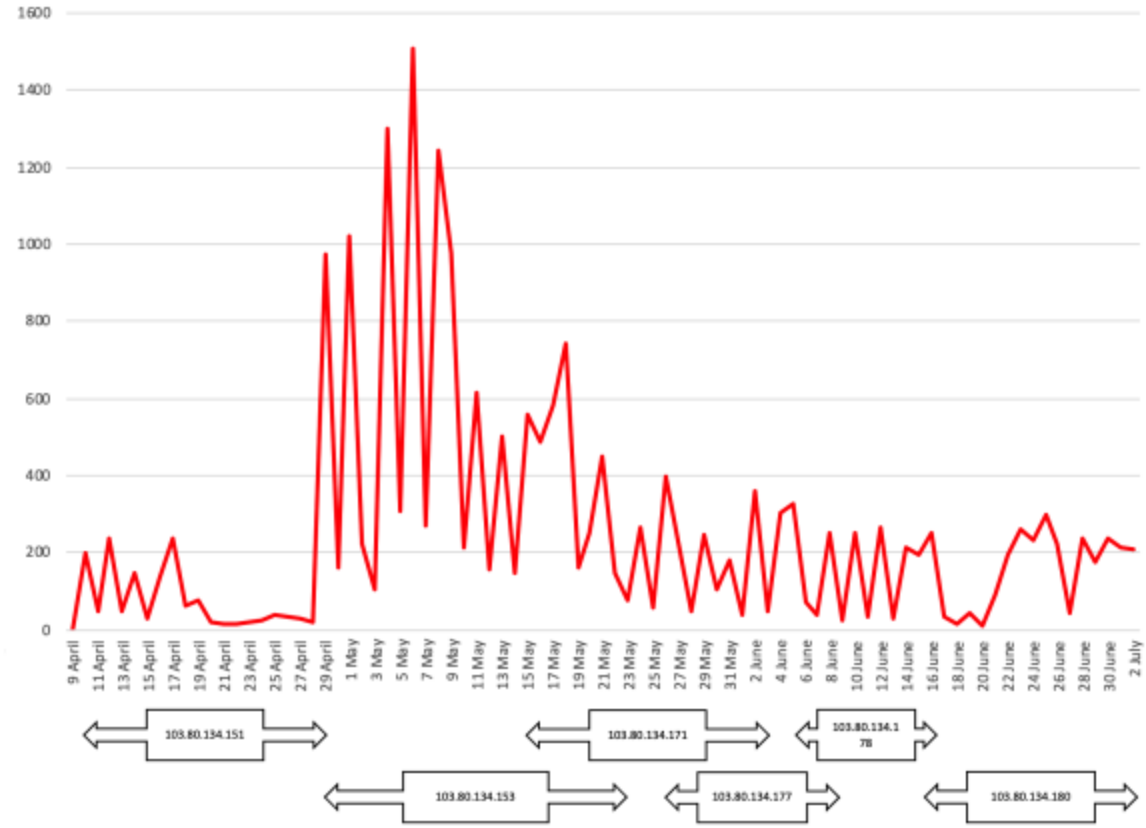


Figure 2: Daily Connections to MoqHao IPs

When we looked more specifically at where these potential victims were located, based on geolocation data, we found communications emanating from across Japan with large clusters focused on the main population centres.

The following figures provide a snapshot of victim locations, at a high level, during the period of analysis – clustered around Tokyo, Kyoto/Osaka/Nagoya and Fukuoka.

Specific details of victim communications have been shared with JPCERT through our outreach team.

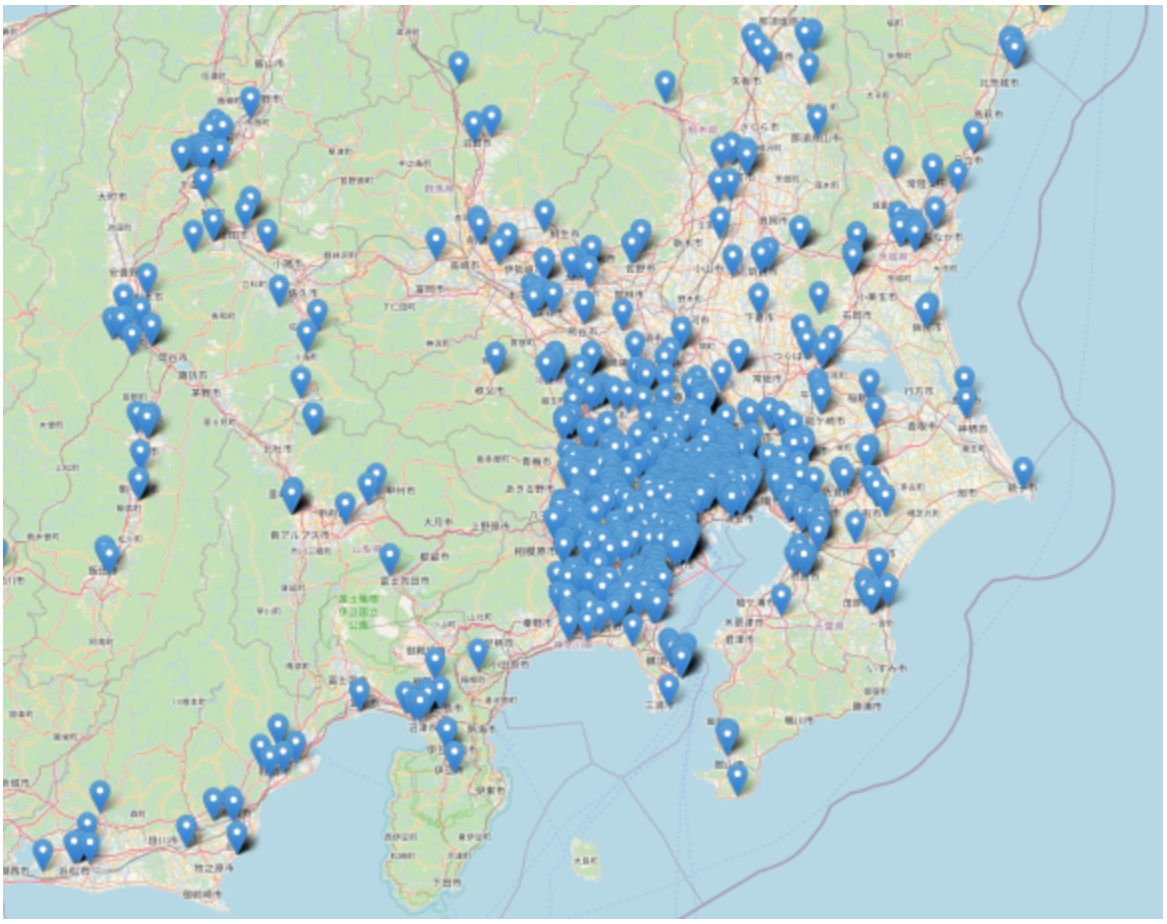


Figure 3: MoqHao Victims – Tokyo

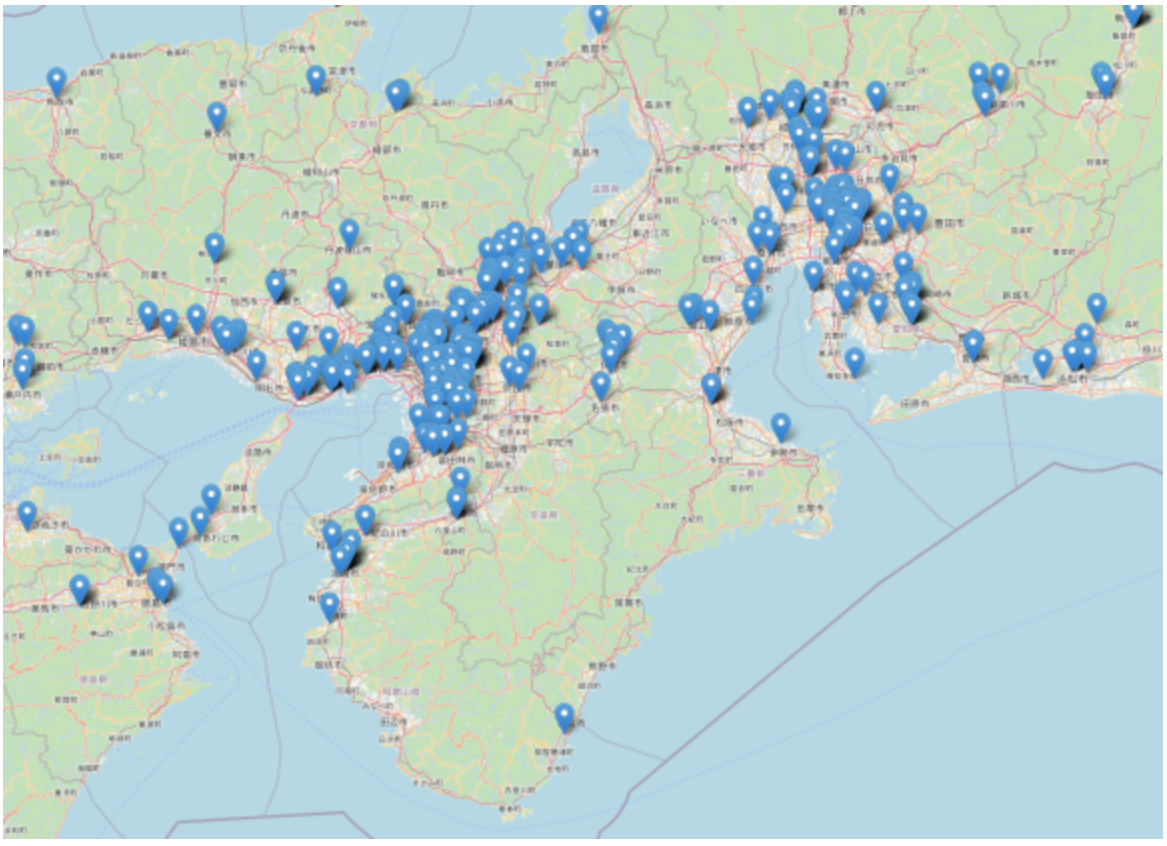


Figure 4: MoqHao Victims – Kyoto/Osaka/Nagoya

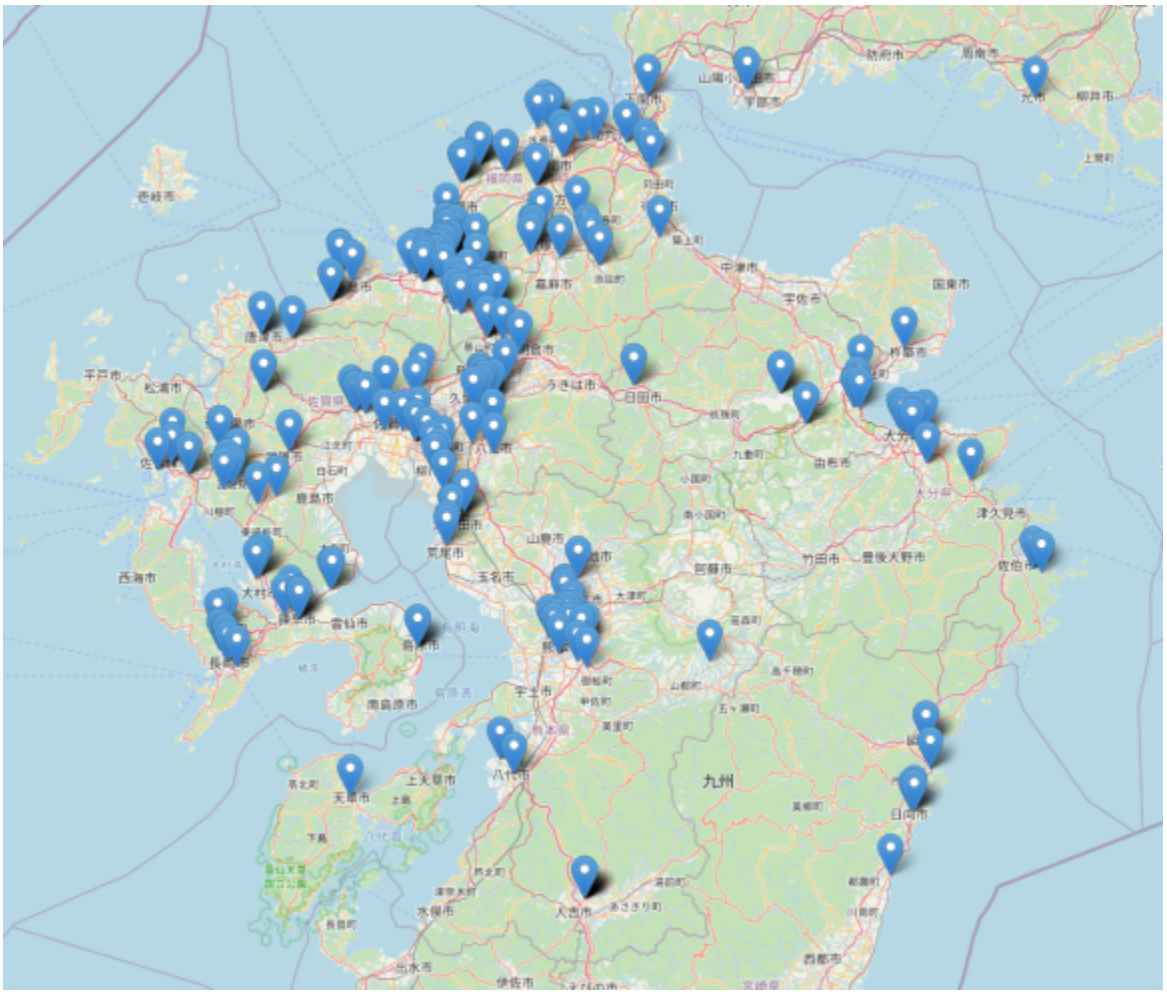


Figure 5: MoqHao Victims – Fukuoka

Conclusion

In this first blog, we have looked at some high-level details of a subset of recent MoqHao campaigns, providing an insight into the consistent nature of the threat actors activities – with victims connecting to distribution servers throughout the analysis period. We have established a minimum number of around 200-300 victim connections per day, based on our coverage of six distribution servers assigned to HDTIDC Limited in South Korea.

We have also hopefully brought to your attention several trustworthy commentators to follow for daily updates on MoqHao indicators.

In future blogs on this subject, we will continue to track the broad trends surrounding MoqHao, as well as diving deeper into the various stages on the malware's network infrastructure.

We welcome any thoughts or feedback through our Twitter page – @teamcymru_s2