1. From the extracted IOCs, outline the type of enrichments that can facilitate cyber threat investigation.

As described in the article, most of the AS originates from China with 4 AS identified belonging to Chinese systems, 1 to Japan and 1 to Philippines.

From the extracted ASN and IP addresses, further exploration of associated domains, subdomains and IP addresses should be carried out to gain a wider understanding of this attack vector.

There should also be an active monitoring of activities within these domains, looking out especially for zone transfers, as it is very likely they the attackers would transfer zones regularly.

All this information can be blacklisted on the SIEM platforms for real-time threat detection. In addition to rule-based logging, a simple n-gram approach to detect randomly generation domains queried from within the network can also be added. This could potentially contextualize the attack and detect similar patterns which could be useful in preventing zero-day attack patterns. Although this is likely to raise a lot of false positives when specifically looking for the Aria-body backdoor, it casts a wide net and further analysis can bring to light the specifics of each attack. Further use of feature engineering could be use to finetune the model to specifically pick up specific attacks.

2. How would you surface potential additional unknown IOCs from this list of IOCs from the report?

One possible way of researching new IOCs is to create an isolated system in which this exploit can safely be allowed. From there, we can log the different packet transactions between victim machines and C&C servers. Understanding the network patterns is crucial in identifying infected hosts since this backdoor requires coordination with C&C to proceed to the final payload. This can be done either by deconstructing the raw packet data or engineering high-level features to be train on supervised models for real-time threat detection.