I'm trying to find a way detecting control channels over ICMP (ICMP shell and others).

As a proposal I would like to detect:

- Unsolicited ECHO Reply
- ECHO Reply with different payload

If there is no such options (I'm pretty sure in it) I will be happy to try and contribute.

In this case I'd like someone experienced to validate the idea details.

---

History

#1 - 09/26/2015 06:21 AM - Victor Julien
You are correct. There is no specific detection for such cases. What do you have in mind?

#2 - 09/26/2015 06:54 AM - Vlad Solontsov
First of all, by detecting I would setup a flow to avoid any additional work for alerting further traffic between src and dest. Just have a rule to alert all the ICMP traffic within a flow.

Secondary, seems like I need a kind of transactions hash-map (I saw this kind of thing in DNS at app level) with a copy of initial Packet.

So, as far as I understand, at registering a module I need to initialize a hash-map (key is to be based on src, dest, id and sequence number). At receiving ECHO Request/Reply try to find and update existing flow.

If no flow,

- for request I need to create a transaction, copy the packet and store the copy in the transaction.
- for reply I need to find a transaction and check the payload.
  - No transaction -- create a flow and raise alert (return 1 from detecting module)
  - Payload mismatch -- create a flow, add initial packet for processing with the flow, update the flow for the current packet (drop the transaction)
  - No mismatch -- just drop the transaction.

Could you please comment how reasonable it is, what are the pitfalls with threading model, etc?

#3 - 10/03/2015 12:34 PM - Vlad Solontsov
Hi,

Sorry for chasing, but is proposal completely wrong?

#4 - 01/01/2016 05:58 PM - Andreas Herz
- Assigned to Anonymous

It's just still in the Queue :)

#5 - 02/23/2019 10:17 PM - Andreas Herz
- Assigned to Community Ticket

#6 - 09/27/2019 01:55 PM - Victor Julien
The flow tracking for (some) ICMP is now done. The rest of the logic will be non-trivial, as ICMP packets are not sent to the app-layer API where the
DNS parser lives.