(U) When the 'Traffic Fairy' Lets You Down

FROM: ▮▮▮▮▮▮▮▮▮▮
Target Development Branch, Yakima Research Station (F921D)
Run Date: 12/14/2005

(C//SI) PINWALE users: If your target seems to have ceased communicating, consider whether it could in fact be a collection, processing or other problem.

(C//SI) Sometimes the normally reliable "traffic fairy" can't or won't deliver your target's text-based data network communications to PINWALE, at least not in a usable form.

(C//SI) When this happens, don't assume that your target is no longer communicating or is no longer accessible. The reasons for missing or "garbled" traffic can vary, but quite often boil down to:

- A. (C//SI) The source of the traffic, usually known as the carrier and labeled with a case notation, has moved, changed characteristics, or gone "off the air" (OTA);

- B. (C//SI) The target itself has changed carriers or communication modes;

- C. (C//SI) The automated processing of the traffic by the SIGINT architecture is being done incorrectly or incompletely;

- D. (S//SI) Your CADENCE selectors may not be hitting due to improper syntax or encoded data; or,

- E. (S//SI) Your CADENCE category's priority in the Forwarding Instruction Table (FIST) is set to a low priority or Priority 6. (Comment: Priority 6 is dependent on another category hitting on the same message with a priority of 1-5 which allows forwarding. If your category is the only category on the message and the priority is 6, the message will not route back to NSAW.)

(U//FOUO) **There are several checks that can easily be performed by you:**

1. (C//SI) Question: Is any traffic from the carrier (case notation) that you used to observe your target on still arriving in PINWALE?

   (S//SI) Answer: If NO and the traffic appears to have "dried up," it could be that the frequency of the carrier has changed, or that the carrier is OTA. Another possibility - the traffic is not being routed in the forwarding thread (example: OUTBLAZE->SCISSORS).

   (U//FOUO) What to Do: Contact your product line's collection support element and the text data flow team.

2. (C//SI) Question: Does the traffic from the target carrier, which once look like it was being processed correctly ("clean"), now look consistently "garbled"?

   (S//SI) Answer: IF YES, it is possible that the protocol stack has changed and/or the sessionizing software (example: WEALTHYCLUSTER/POWERPLANT) is encountering processing problems.

   (C//SI) What to Do: Contact your product line's collection support element.

3. (S//SI) Question: Are the traffic selectors (CADENCE dictionary terms) still adequate for your target?

   (S//SI) Answer: Remember - just because your PINWALE retrieval strategy has been

kept up-to-date doesn't mean that your CADENCE selectors have been given the same consideration.

(S//SI) What to Do: Examine your CADENCE dictionary category and FIST priority, update if necessary, and be careful not to rely on another TOPI's keywords to deliver your traffic to PINWALE.

(C//SI) Assuming everything else is in order, it could be that your target has simply moved to another carrier, or another mode of communicating.

(S//SI) An example is in order. When attempting to reacquire access to passenger airline reservations out of Central America, a candidate IP carrier was placed on mission coverage with every expectation that travel reservation traffic would once again result.

(S//SI) Alas, nothing arrived in PINWALE from this new tasking except what appeared to be an occasional "garbled" session - certainly nothing like what was expected. The body of a typical session appeared as:

```
*eoc2c
[????a???????@???a???@@@????@@@@????@@@@?????@???a???@@@@????@@@?????@???a??@@
@@@????@@@?????@???a???@@@@????@@@????@@@@?????@@???@@????@@@@????
@@@@@
@@@@@@@@@@??@@@@@?@????@????@@@@@@@??@@@????@@@????@@@@@???
@@@@??@???@@@?
?@????@????@@@@@@??@@@????@@????@@@@?@???@\\\\?nN??????????????`????
?,?a??`????@????nN?????????
*eotxt
```

(S//SI) Upon further evaluation, it was discovered that the old IBM EBCDIC character set was being used within the target carrier - not the expected ASCII. As a result, no CADENCE keywords were hitting in the body of the traffic, and only an occasional hit occurred on the metadata.

(S//SI) Once the front-end processing software had been updated, the session above appeared as:

```
**eoc2c
B-SINE COMPLETE/18AUG/PD
>+/$0804/18AUG
P BAQ/OUT 419P FDC
P BAQ/OFF 432P FDC
P PTY/ON 523P FDC
P PTY/ETA 530P FDC
SKED BAQ ORIG 440P GTD 2 SHIP 372
PTY 555P 730P GTA 14 GTD 15 SHIP 376
JFK 143A TERM 1 GTA ****
B-SINE OUT
*eotxt
```

(S//SI) Only after the software fix did the traffic from this carrier start hitting on CADENCE target keywords within the body of traffic sessions. Not only that, this fix resulted in a corporate solution for future similar situations.

(S//SI) Normally, a collection site would notice that a carrier is OTA right away and initiate a search for its replacement (or movement). S33 mission management would also be notified, and the tasking TOPIs would receive word from them. However, not every target analyst that might care will receive notification.

(S//SI) As you know, a communications channel might have a single TOPI or two on its SURREY tasker, yet result in hundreds of reports by over a dozen different product lines over the course of a year. Several of these target analysts might simply think their targets had stopped communicating - it could be some time before they bother to see if their source had dried up.

Especially since a single carrier is rarely the sole source for a given target set.

(S//SI) **The bottom line is, if you have tried everything, and nothing seems to work, contact your collection support element and let them know you have lost your target.** The appropriate SIGDEV element(s) and [S33](#) mission managers will be engaged from there. In any case, these folks should be able to help you correctly identify the problem and help you reacquire access to your target's communications in usable form.

(S//SI) SPECIAL NOTE: In those instances where your targets seem to have suddenly disappeared from carriers collected by Yakima Research Station (YRS aka JACKKNIFE at USF-787), we in the YRS target development branch are also here to help and advise. You can contact us at ████@yrs.f.nsa or ████████