IODEF Extensions for Phishing and Other E-Crimeware

Patrick Cain

Latest Status

- New draft out.
  - Missed deadline by a little; should show up in repository soon.
  - draft-ietf-inch-phishingextns-02
    - One Technical change
    - Many editorial modifications

Technical Change

- A text string field was added to the ‘phish:Source’ data item.
  - Capture DNS/whois data at the time of the initial investigation.
- When investigating an incident, current DNS/whois data is used. That data changes as the incident progresses. One may find the (fraudulent) DNS data changes from time to time.

The future

- Add a few more examples to the appendix
  - Fix any bugs detected
- Generating a few more tools to encode/process data
  - We have generated and sent phish reports to the APWG repository via XML. ☺
- Await comments

End

Patrick Cain
pcain@coopercain.com