IODEF Extensions for Phishing and Other E-Crimeware

Patrick Cain

Latest Status

- New draft out.
  - draft-ietf-inch-phishingextns-03
    - A bunch of Technical changes
    - Many editorial modifications
    - (as of Today) I don’t know of any bugs.

Technical Changes

- Added a LureSource Element
  - DNS/Domain info to Source ID
  - Added RegistryKey and DownloadedFiles fields
- Added field to support including malware
  - A binary field with an optional mask
  - A hash of the binary
- Fixed a bunch of things related to -070
- Radically changed the email inclusion section
- Lots of XML corrections…

Related stuff

- Generated a bunch of sample/test/etc reports to make sure that we could convey everything we wanted in a report
  - Phish report
  - Spam report
  - Virus report
- My tools participated in the interop. ☺

The future

- Add a few more examples to the appendix
- Fix any bugs detected
- Await comments

- Generate an -04 and do a LC
  - Right after iodef-07 goes to LC

End

Patrick Cain
pcain@coopercain.com