INCH Extensions for Phishing

Pat Cain

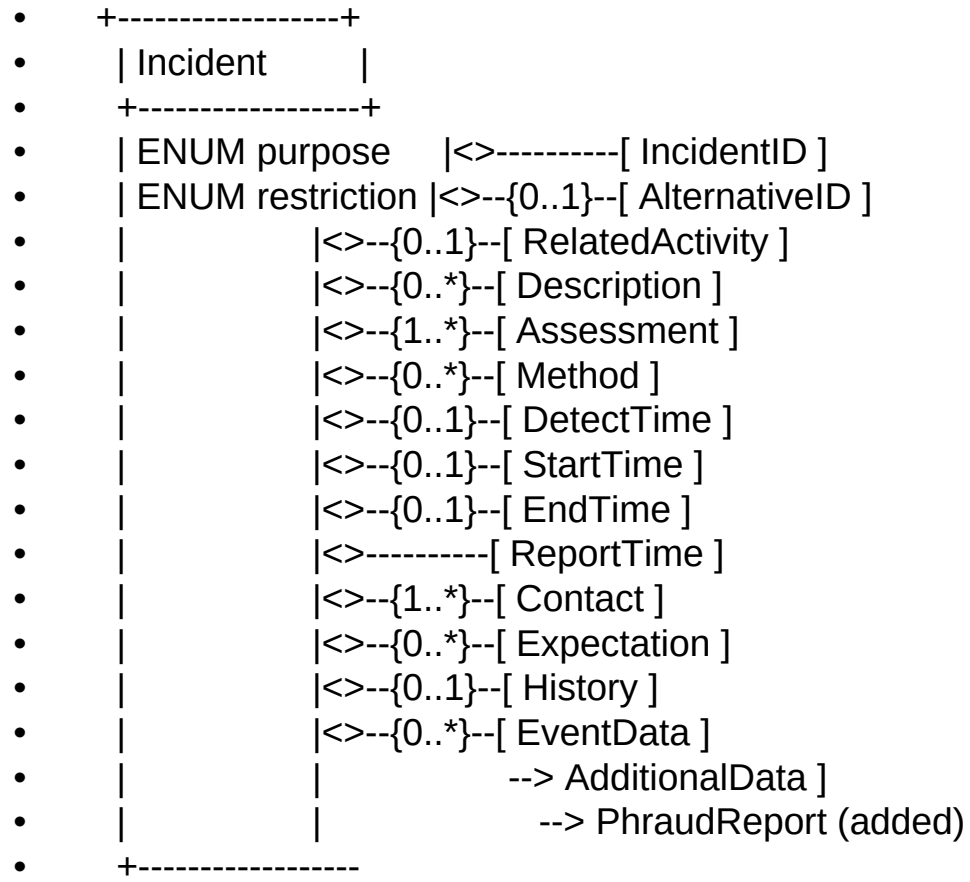
pcain@coopercain.com

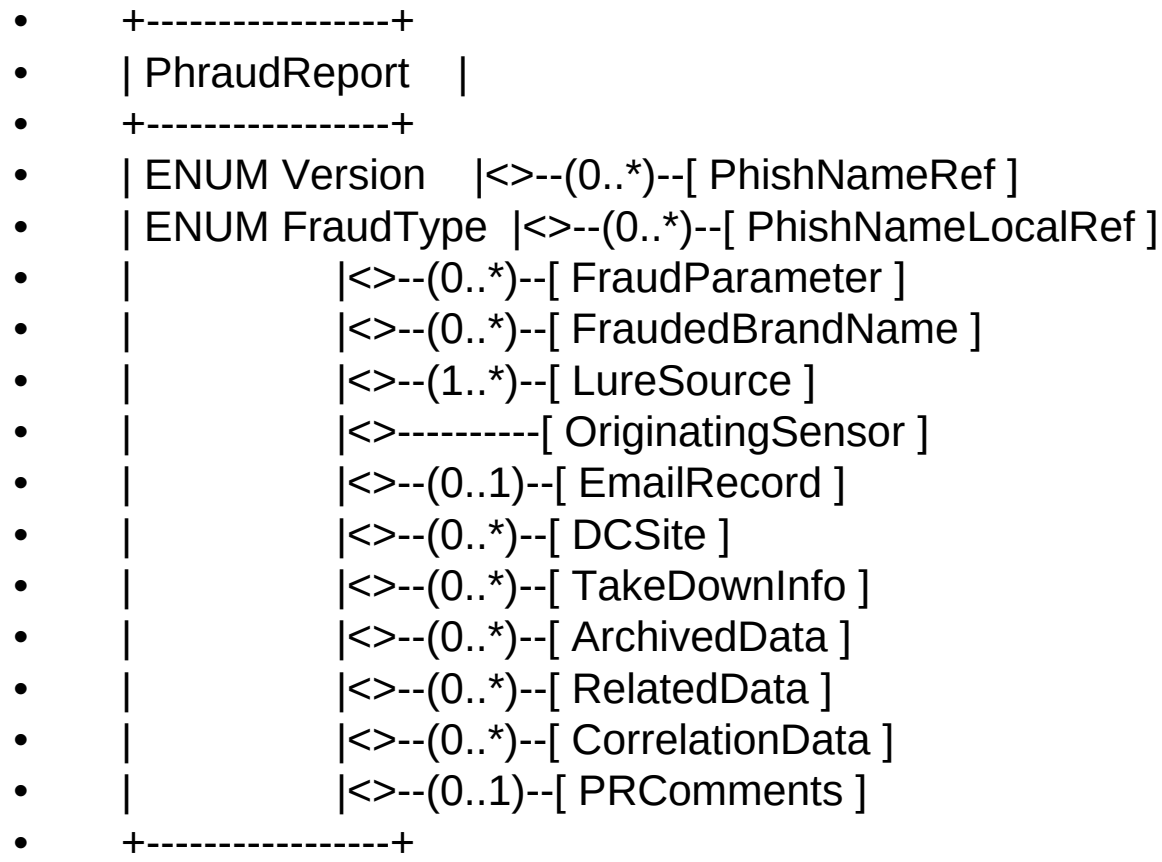
Draft-ietf-inch-phishingextns-01

- WG accepted doc in Minnesota
- Draft -00 came out early June
- -01 came out early July
- -02 should come out mid-August

Mods from jevans-00 to -00

- Fixed the DTD and the Schema
- Moved PhraudReport from top-level to EventData
- Added support for:
  - other e-fraud
  - malware
  - basic large-scale spam reporting
- Added more words


+-----------------+
| Incident |
+-----------------+
| ENUM purpose |<>----------[IncidentID]
| ENUM restriction |<>--{0..1}--[AlternativeID]
| |<>--{0..1}--[RelatedActivity]
| |<>--{0..*}--[Description]
| |<>--{1..*}--[Assessment]
| |<>--{0..*}--[Method]
| |<>--{0..1}--[DetectTime]
| |<>--{0..1}--[StartTime]
| |<>--{0..1}--[EndTime]
| |<>----------[ReportTime]
| |<>--{1..*}--[Contact]
| |<>--{0..*}--[Expectation]
| |<>--{0..1}--[History]
| |<>--{0..*}--[EventData]
| | --> AdditionalData]
| | --> PhraudReport (added)
+-----------------


+----------------+
| PhraudReport |
+----------------+
| ENUM Version |<>--(0..*)--[PhishNameRef]
| ENUM FraudType |<>--(0..*)--[PhishNameLocalRef]
| |<>--(0..*)--[FraudParameter]
| |<>--(0..*)--[FraudedBrandName]
| |<>--(1..*)--[LureSource]
| |<>----------[OriginatingSensor]
| |<>--(0..1)--[EmailRecord]
| |<>--(0..*)--[DCSite]
| |<>--(0..*)--[TakeDownInfo]
| |<>--(0..*)--[ArchivedData]
| |<>--(0..*)--[RelatedData]
| |<>--(0..*)--[CorrelationData]
| |<>--(0..1)--[PRComments]
+----------------+

Modes from -00 to -01

- Fixed the DTD and the Schema
- Checked consistently in DTD/Schema/Words

Modes from -01 to -02

- Fix the DTD and the Schema