Phishing Reports using the INCH Format

Pat Cain
The Cooper-Cain Group

09 March 2005
IETF #62

Some History

- The Financial Services Technology Consortium (www.fstc.org) ran a counter-phishing project last fall
- The AntiPhishing Working Group (www.antiphishing.org) collaborated
- Roughly ~20 banks, some FIs, and about 50 vendors participated

Phishing

- One of our successes was to agree on a definition ☺

  “Phishing is a broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt to trick individuals into revealing personal credentials that can be used fraudulently.”

The current state of the world

- Many products help/hurt phish detection, reporting and forensics
  - Every one has a different reporting format
  - Every one reports to a different place
  - Very hard to do metrics
  - Very hard to see if your brand is being phished

Relation to INCH

- Everyone agreed that we needed a common format to gather “activity” information
- I suggested that we create some extensions to the INCH format for phishing
  - We don’t need to reinvent the format
  - It uses XML, which will obviously save the world
  - There is some tool support.

Draft-jevans-phishing-xml

- A doc popped out
  - Currently not a WG doc
- We created two extensions to inch-03
- Phishing Report – ext to Additional Data
  - Includes phishing type of stuff not already covered
- PhishRecord – ext to Record Data
  - Mostly forensic data

PhishingReport

- Record information for a specific attack/exploit
  - Type of phishing trip
  - Brand name phished
  - Copy of lure
  - Credential collector Site
  - Takedown info, if known

PhishingReport Structure

```
+---------------------------+
|  EventData.AdditionalData |
+---------------------------+
| ENUM type (9 = xml)       |<>---------[ PhishingReport     ]
| STRING meaning (xml)      |
+---------------------------+

+------------------------+
| PhishingReport         |
+------------------------+
| ENUM Version           |<>--(0..*)--[ PhishParameter      ]
| ENUM PhishType         |----(0..*)--[ PhishedBrandName    ]
|                        |<>--(0..*)--[ DataCollectionType  ]
|                        |<>--(0..*)--[ DataCollectionSite  ]
|                        |<>----------[ OriginatingSensor   ]
|                        |<>--(0..*)--[ TakeDownInfo        ]
|                        |<>--(0..*)--[ ArchivedData        ]
|                        |<>--(0..*)--[ RelatedSites        ]
|                        |<>--(0..*)--[ CorrelationData     ]
|                        |----(0..1)--[ Comments            ]
+------------------------+
```

PhishRecord

- Record ‘forensical’ information relevant to a specific phish attempt:
  - Email headers, content, IP information
  - Looks a lot like a spam complaint

PhishRecord Structure

```
+-----------------------+
| RecordItem            |
+-----------------------+
| ANY (PhishRecord)     |
| ENUM Type (xml)       |
+-----------------------+

+-----------------------+
| PhishRecord           |
+-----------------------+
|                       |<>--(0..*)---[ EmailOriginatorIP  ]
|                       |<>--(0..*)---[ EmailHeader        ]
|                       |<>--(0..*)---[ EmailBody          ]
|                       |<>--(0..*)---[ EmailComments      ]
+-----------------------+
```

Status of -00

- The DTD and Schema comply with -03
  - Including the -03 bugs
- When our report generator works, we'll put out an -01 and a new doc and schema/dtd
- Docs are at www.coopercain.com/incidents

Status

- -00 went out Jan 03, 2005
- -01 should be out soon.
  - We were requested to add some spam-specific elements
- The goal is to have some tools this spring and start using it by mid-year.
  - Using == APWG accepts reports in this format
  - Some vendors will support it.

Our Request for Help

- If you are interested in this topic, we take comments ☺
- I’m sure that the XML (and iodef-extension) is broken.
- I’m sure we won’t be the only people to craft extensions, so I want to get it right.