MILE Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2014

P. Kampanakis
Cisco Systems

October 18, 2013

IODEF Usage Guidance
draft-pkampana-iodef-guidance-00

Abstract

The Incident Object Description Exchange Format [RFC5070] defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. Since the IODEF model includes a wealth of available options that can be used to describe a security incident or issue, it can be challenging for implementers to develop tools that can Leverage IODEF for incident sharing. This document provides guidelines for IODEF implementers. It will also address how common security indicators can be represented in IODEF. The goal of this document is to make IODEF's adoption by vendors easier and encourage faster and wider adoption of the model by Computer Security Incident Response Teams (CSIRTs) around the world.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2014.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Implementation Strategy 3
3.1. Recommended classes to implement 4
3.2. Decide what IODEF will be used for 4
4. IODEF considerations and how to address them 4
4.1. Unnecessary Fields 4
4.2. External References 4
4.3. Extensions 5
4.4. Logic for watchlist of indications 5
4.5. Externally defined Indicators 6
4.6. Restrictions in IODEF 6
5. Current uses of IODEF 6
5.1. Anti-Phishing Working Group 6
5.2. Inter-vendor and Service Provider Exercise 7
5.3. Collective Intelligence Framework 7
5.4. Other 8
6. Security Considerations 8
7. Acknowledgements 8
8. Security Considerations 8
9. References 8
9.1. Normative References 8
9.2. Informative References 8
Appendix A. Inter-vendor and Service Provider Exercise Examples 9
A.1. DDoS 9
A.2. Malware 11
A.3. Spear-Phishing 16
Author's Address 19

1. Introduction

The Incident Object Description Exchange Format in [RFC5070] defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents. The IODEF data model consists of multiple classes and data types that are used in the IODEF XML schema.

The IODEF schema was designed to be able to describe all the possible fields that would be needed in a security incident exchange. Thus, IODEF contains plenty data constructs that could potentially make it harder for IODEF implementers to decide which are the most important ones. Additionally, in the IODEF schema, there exist multiple fields and classes which do not necessarily need to be used in every possible data exchange. Moreover, there are fields that are useful only in data exchanges of non-traditional security events. This document tries to address the issues above. It will also address how common security indicators can be represented in IODEF. It will point out the most important IODEF classes for an implementer and describe other ones that are not as important. Also, it addresses some common challenges for IODEF implementers and how they should be addressed. The end goal of this document is to make IODEF's adoption by vendors easier and encourage faster and wider adoption of the model by Computer Security Incident Response Teams (CSIRTs) around the world.

Section 3 discusses the recommended classes and how an IODEF implementer should chose the classes to implement. Section 4 presents common considerations and implementer will come across and how to address them. Section 5 goes over some basic security concepts and how they can be expressed in IODEF.

2. Terminology

The terminology used in this document follows the one defined in RFC 5070 [RFC5070] and I-D.draft-ietf-mile-sci [I-D.ietf-mile-sci].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Implementation Strategy

It is important for IODEF implementers to be able to distinguish how the IODEF classes will be used for incident information exchanges.

It is critical for an implementer to follow a strategy according to which he will chose to implement various IODEF classes. It is also important to know what the most common classes that will be used to describe common security incident or indicators. Thus, this section will describe the most important classes and factors an IODEF implementer should take into consideration before designing the implementation or tool.

3.1. Recommended classes to implement

This section explains the mandatory to implement IODEF classes that are required more than once and also are useful.

[...More to be added...]

3.2. Decide what IODEF will be used for

This section describes that there is no need to implement all fields of IODEF, the ones that are necessary for your use-cases. The implementer should look into the schema and decide classes to implement (or not) Also it explains that other external schemata might be needed to describe incidents or indicators, based on SCI draft extensions.

[...More to be added...]

4. IODEF considerations and how to address them

4.1. Unnecessary Fields

This section talks about fields that do not always play in important role like Assessment, Impact

[...More to be added...]

4.2. External References

draft draft-montville-mile-enum-reference-format "This format allows the <Version> to be associated with the id rather than the id_type. By requiring that a specific type and version be associated with the identifier, an implementer can look up the type in an IANA table to understand exactly what the identifier in ReferenceName is and how s/he may expect that identifier to be structured."

[...More to be added...]

4.3. Extensions

This section explains how to describe things IODEF can't describe ([I-D.ietf-mile-sci] draft), or extensions not yet known, or implemented, when do you use another xml schema encapsulated in iodef

[...More to be added...]

4.4. Logic for watchlist of indications

Multiple indicators occasionally need to be combined in an IODEF document. For example, a botnet might have multiple command and control servers. A consistent predicate logic should be followed in order to present such relationships in IODEF.

In [RFC5070], predicate logic only consisted of logical AND. For example, if an Flow Class contained two System classes with "source" and "destination" as category attributes, it was assumed that both Systems should be present in order for the Flow to be true and thus marked as an indicator.

[I-D.ietf-mile-rfc5070-bis] defines two new category attributes in the System Class that can enhance the IODEF predicate logic functionality. These are watchlist-source and watchlist-destination and they serve for watchlist indicator groupings. When a Flow Class that consists of multiple Systems with watchlist-source and watchlist-destination attributes (watchlist of Systems) the System information should be ORed for the Flow Class described. In other words, either System description should be considered as a watchlist indicator. The content in the EventData Class the Node belongs to should be combined with the watchlist of Systems using AND logic. Different Flow classes that consist of different System classes (with watchlist-source or destination as attributes) follow AND logic in their parent EventData Class.

IODEF's grouping predicate logic follows the above pattern consistently. [I-D.ietf-mile-rfc5070-bis] defined the HashInformation Class that describes a file hash information as also described in [RFC5901]. The HashInformation Class is of HashSigDetails type which consists of elements that describe the file hash details. Some of the attributes of the HashSigDetails are introduced to describe watchlist groupings (i.e. PKI_email_ds_watchlist, PGP_email_ds_watchlist, file_hash_watchlist, email_hash_watchlist). If any of these attributes are used in two or more HashInformation Classes of a Record then HashInformation content is ORed for the Record. For example, if two HashInformation types are set to file_hash_watchlist, the list of hash details provided are just alternate representations for the same hash (SHA256. SHA1 etc).

Similarly, if multiple HashInformation classes, with "watchlist" in their category attribute, are in a Record using Reference elements or others, they should all be treated as different representations of the same file hash, assuming the FileName element is not used in the HashInformation.

In some cases the predicate logic in IODEF can slightly change. [I-D.ietf-mile-rfc5070-bis] introduces the WindowsRegistryKeyModified Class which is of type RegistryKeyModified. RegistryKeyModified has an optional type attribute which has watchlist as an option in order to include the ability to group WindowsRegistryKeyModified. In order to group multiple WindowsRegistryKeyModified of the same watchlist of indicators multiple WindowsRegistryKeysModified should be used in the same RecordData or EventData Class. If the RegistryKeyModified Classes are not under the same RecordData or EventData Class they should be treated as different indicator Keys modified.

4.5. Externally defined Indicators

set-uid,uid and its use with SCI draft [I-D.ietf-mile-sci]

[...More to be added...]

4.6. Restrictions in IODEF

This section describes how Restriction can pose challenges

[...More to be added...]

5. Current uses of IODEF

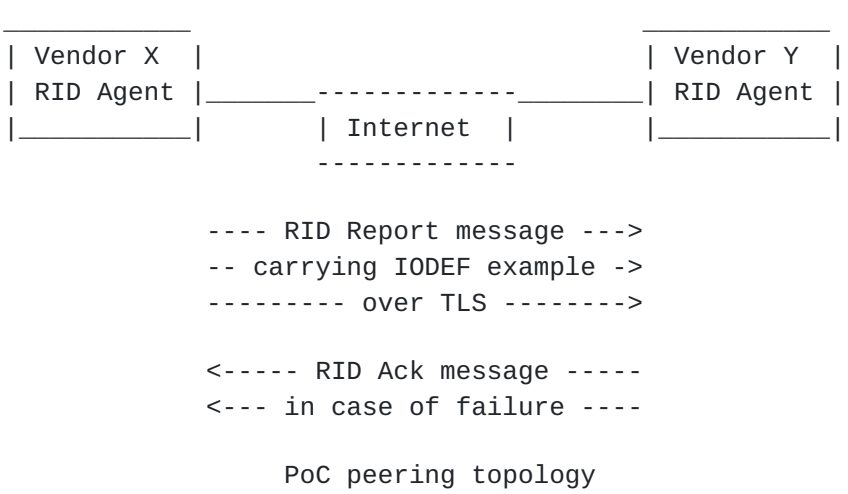
IODEF is currently used by various organizations in order to represent security incidents and share incident and threat information between security operations organizations.

5.1. Anti-Phishing Working Group

The Anti-Phishing Working Group ([APWG]) is using [RFC5070] to represent email phishing information. [APWG] also uses IODEF to aggregate and share Bot and Infected System Alerting and Notification System (BISANS) and Cyber Bullying IODEF records. Special IODEF extensions are used in order to mark the sensitivity of the exchanged information. Shared infected system or email phishing records can then be used by interested parties in order to provide mitigations. [APWG] leverages tools of its eCRISP-X toolkit in order to share and report e-Crime IODEF records.

5.2. Inter-vendor and Service Provider Exercise

Various vendors organized and executed an exercise where multiple threat indicators were exchanged using IODEF. The transport protocol used was RID. The threat information shared included incidents like DDoS attacks. Malware and Spear-Phishing. As this was a proof-of-concept (PoC) exercise only example information (no real threats) were shared as part of the exchanges.



PoC peering topology

The figure above shows how RID interactions took place during the PoC. Participating organizations were running RID Agent software on-premises. The RID Agents formed peering relationships with other participating organizations. When Entity X had a new incident to exchange it would package it in IODEF and send it to Entity Y over TLS in a RID Report message. In case there was an issue with the message, Entity Y would send an RID Acknowledgement message back to Entity X which included an application level message to describe the issue. Interoperability between RID agents and the standards, [RFC6545] and [RFC6546], was also proven in this exercise. Appendix A includes some of the incident IODEF example information that was exchanged by the organizations' RID Agents as part of this proof-of-concept.

5.3. Collective Intelligence Framework

The Collective Intelligence Framework [CIF] is a cyber threat intelligence management system that uses IODEF to combine known malicious threat information from multiple sources and use that it to identify, detect and mitigate. The threat intelligence can be IP addresses, domains and URLs that are involved in malicious activity. IODEF records can be consumed by a CIF standalone client or CIF browser plugins that a user can use to make informed decisions about

threat information.

5.4. Other

IODEF is also used in various projects and products to consume and share security information. Various vendor incident reporting products have the ability to consume and export in IODEF format. Perl and Java modules exist in order to parse IODEF documents and their extensions. Additionally, some worldwide CERT organizations are already able to use receive incident information in IODEF.

6. Security Considerations

7. Acknowledgements

8. Security Considerations

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.

[RFC5901] Cain, P. and D. Jevans, "Extensions to the IODEF-Document Class for Reporting Phishing", RFC 5901, July 2010.

[RFC6545] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6545, April 2012.

[RFC6546] Trammell, B., "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS", RFC 6546, April 2012.

9.2. Informative References

[APWG] "APWG", <http://apwg.org/>.

[CIF] "CIF", <https://code.google.com/p/collective-intelligence-framework/wiki/WhatisCIF>.

[I-D.ietf-mile-rfc5070-bis]
Danyliw, R. and P. Stoecker, "The Incident Object Description Exchange Format", draft-ietf-mile-rfc5070-bis-00 (work in progress), May 2013.

[I-D.ietf-mile-sci]
Takahashi, T., Landfield, K., Millar, T., and Y. Kadobayashi, "IODEF-extension for structured cybersecurity information", draft-ietf-mile-sci-08 (work in progress), July 2013.

Appendix A. Inter-vendor and Service Provider Exercise Examples

Below some of the incident IODEF example information that was exchanged by the vendors as part of this proof-of-concept Inter-vendor and Service Provider Exercise.

A.1. DDoS

```
<?xml version="1.0" encoding="UTF-8"?>
<IODEF-Document version="1.00" lang="en"
    xmlns="urn:ietf:params:xml:ns:iodef-1.41"
    xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.41"
    xmlns:iodef-sci="urn:ietf:params:xml:ns:iodef-sci-1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <iodef:Incident purpose="reporting" restriction="default">
         <iodef:IncidentID name="csirt.example.com">
             189701
         </iodef:IncidentID>
         <iodef:StartTime>2013-02-05T00:34:45+00:00</iodef:StartTime>
         <iodef:DetectTime>2013-02-05T01:15:45+00:00</iodef:DetectTime>
         <iodef:ReportTime>2013-02-05T01:34:45+00:00</iodef:ReportTime>
         <iodef:description>DDoS Traffic Seen</iodef:description>
            <iodef:Assessment occurrence="actual">
                <iodef:Impact severity="medium" type="dos">
                DDoS Traffic</iodef:Impact>
                <iodef:Confidence rating="numeric">90
                </iodef:Confidence>
            </iodef:Assessment>
            <iodef:Contact role="creator" type="organization">
                <iodef:ContactName>Dummy Test</iodef:ContactName>
                <iodef:Email>contact@dummytest.com</iodef:Email>
            </iodef:Contact>
            <iodef:EventData>
```

```
               <iodef:Description>
                   Dummy Test sharing with ISP1
               </iodef:Description>
            <iodef:Expectation action="other"/>
            <iodef:Method>
               <iodef:Reference>
                  <iodef:ReferenceName>
                      Low Orbit Ion Cannon User Agent
                  </iodef:ReferenceName>
                  <iodef:URL>
                     http://blog.spiderlabs.com/2011/01/loic-ddos-
                     analysis-and-detection.html
                  </iodef:URL>
                  <iodef:URL>
                     http://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon
                  </iodef:URL>
               </iodef:Reference>
            </iodef:Method>
            <iodef:Flow>
               <iodef:System category="watchlist-source" spoofed="no">
                  <iodef:Node>
                    <iodef:Address category="ipv4-addr">
                       10.10.10.104</iodef:Address>
                  </iodef:Node>
                  <iodef:Node>
                    <iodef:Address category="ipv4-addr">
                       10.10.10.106</iodef:Address>
                                  </iodef:Node>
                  <iodef:Node>
                    <iodef:Address category="ipv4-net">
                     1172.16.66.0/24</iodef:Address>
                     </iodef:Node>
                  <iodef:Node>
                    <iodef:Address category="ipv6-addr">
                     2001:db8:dead:beef::</iodef:Address>
                                </iodef:Node>
   <iodef:Service ip_protocol="6">
      <iodef:Port>1337</iodef:Port>
      <iodef:Application user-agent="Mozilla/5.0 (Macintosh; U;
             Intel Mac OS X 10.5; en-US; rv:1.9.2.12) Gecko/
             20101026 Firefox/3.6.12">
      </iodef:Application>
   </iodef:Service>
              </iodef:System>
               <iodef:System category="target">
                  <iodef:Node>
                    <iodef:Address category="ipv4-addr">
   10.1.1.1</iodef:Address>
```

```
                </iodef:Node>
                <iodef:Service ip_protocol="6">
                  <iodef:Port>80</iodef:Port>
                </iodef:Service>
              </iodef:System>
              <iodef:System category="sensor"><iodef:Description>
                  Information provided in FLow class instance is from
                  Inspection of traffic from network tap
              </iodef:Description></iodef:System>
            </iodef:Flow>
         </iodef:EventData>
     </iodef:Incident>
 </IODEF-Document>
```

A.2. Malware

```
        <?xml version="1.0" encoding="UTF-8"?>
                  <iodef:IODEF-Document xmlns:ds="
                      http://www.w3.org/2000/09/xmldsig#"
                      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.41">
             <iodef:Incident purpose="reporting">
               <iodef:ReportID name="EXAMPLE CIRT">
                  189234
               </iodef:ReportID>
               <iodef:ReportTime>
                  2013-03-07T16:14:56.757+05:30
               </iodef:ReportTime>
               <iodef:Description>
                  Malware and related indicators identified
               </iodef:Description>
               <iodef:Assessment occurrence="potential">
                 <iodef:Impact severity="medium" type="info-leak">
                    Malware with Command and Control Server
                    and System Changes
                 </iodef:Impact>
               </iodef:Assessment>
               <iodef:Contact role="creator" type="organization">
                 <iodef:ContactName>EXAMPLE CIRT</iodef:ContactName>
                 <iodef:Email>emccirt@emc.com</iodef:Email>
               </iodef:Contact>
               <iodef:EventData>
                 <iodef:Method>
                   <iodef:Reference>
                     <iodef:ReferenceName>Zeus</iodef:ReferenceName>
                     <iodef:URL>
                         http://www.threatexpert.com/report.aspx?
                         md5=e2710ceb088dacdcb03678db250742b7
```

```
      </iodef:URL>
    </iodef:Reference>
  </iodef:Method>
  <iodef:Flow>
    <iodef:System category="watchlist-source">
      <iodef:Node>
        <iodef:Address category="ipv4-addr">
           192.168.2.200
        </iodef:Address>
        <iodef:Address category="site-uri">
           http://zeus.556677889900.com/log-bin/
           lunch_install.php?aff_id=1&amp;amp;
           lunch_id=1&amp;amp;maddr=&amp;amp;
           action=install
        </iodef:Address>
        <iodef:NodeRole attacktype="c2-server"/>
      </iodef:Node>
    </iodef:System>
  </iodef:Flow>
  <iodef:Record>
    <iodef:RecordData>
      <iodef:HashInformation>
        <ds:Reference>
          <ds:DigestMethod Algorithm="
             http://www.w3.org/2001/04/xmlenc#sha1"/>
          <ds:DigestValue>
               MHg2NzUxQTI1MzQ4M0E2N0Q4NkUwRjg0NzYwRj
               YxRjEwQkJDQzJFREZG</ds:DigestValue>
        </ds:Reference>
      </iodef:HashInformation>
      <iodef:HashInformation>
        <ds:Reference>
          <ds:DigestMethod Algorithm="
              http://www.w3.org/2001/04/xmlenc#md5"/>
          <ds:DigestValue>
              MHgyRTg4ODA5ODBENjI0NDdFOTc5MEFGQTg5NTE
              zRjBBNA==
          </ds:DigestValue>
        </ds:Reference>
      </iodef:HashInformation>
      <iodef:WindowsRegistryKeysModified>
        <iodef:Key registryaction="add_value">
          <iodef:KeyName>
              HKLM\Software\Microsoft\Windows\
              CurrentVersion\Run\tamg
          </iodef:KeyName>
          <iodef:Value>
             ?\?\?%System%\wins\mc.exe\?\??
```

```
                    </iodef:Value>
                  </iodef:Key>
                  <iodef:Key registryaction="modify_value">
                    <iodef:KeyName>HKLM\Software\Microsoft\
                       Windows\CurrentVersion\Run\dqo
                    </iodef:KeyName>
                    <iodef:Value>"\"\"%Windir%\Resources\
                        Themes\Luna\km.exe\?\?"
                    </iodef:Value>
                  </iodef:Key>
                </iodef:WindowsRegistryKeysModified>
              </iodef:RecordData>
            </iodef:Record>
          </iodef:EventData>
          <iodef:EventData>
            <iodef:Method>
              <iodef:Reference>
                <iodef:ReferenceName>Cridex</iodef:ReferenceName>
                <iodef:URL>
                    http://www.threatexpert.com/report.aspx?
                    md5=c3c528c939f9b176c883ae0ce5df0001
                </iodef:URL>
              </iodef:Reference>
            </iodef:Method>
            <iodef:Flow>
              <iodef:System category="watchlist-source">
                <iodef:Node>
                  <iodef:Address category="ipv4-addr">
                     10.10.199.100
                  </iodef:Address>
                  <iodef:NodeRole attacktype="c2-server"/>
                </iodef:Node>
                <iodef:Service ip_protocol="6">
                  <iodef:Port>8080</iodef:Port>
                </iodef:Service>
              </iodef:System>
            </iodef:Flow>
            <iodef:Record>
              <iodef:RecordData>
                <iodef:HashInformation>
                  <ds:Reference>
                    <ds:DigestMethod Algorithm="
                       http://www.w3.org/2001/04/xmlenc#sha1"/>
                    <ds:DigestValue>
                       MHg3MjYzRkUwRDNBMDk1RDU5QzhFMEM4OTVBOUM
                       1ODVFMzQzRTcxNDFD
                    </ds:DigestValue>
                  </ds:Reference>
```

```
                    <ds:Reference>
                      <ds:DigestMethod Algorithm="
                         http://www.w3.org/2001/04/xmlenc#md5"/>
                      <ds:DigestValue>MHg0M0NEODUwRkNEQURFNDMzMEE1
                         QkVBNkYxNkVFOTcxQw==</ds:DigestValue>
                    </ds:Reference>
                  </iodef:HashInformation>
                  <iodef:HashInformation>
                    <ds:Reference>
                      <ds:DigestMethod Algorithm="
                          http://www.w3.org/2001/04/xmlenc#md5"/>
                      <ds:DigestValue>MHg0M0NEODUwRkNEQURFNDMzMEE
                          1QkVBNkYxNkVFOTcxQw==</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference>
                      <ds:DigestMethod Algorithm="http://www.w3.org/
                          2001/04/xmlenc#sha1"/>
                      <ds:DigestValue>MHg3MjYzRkUwRDNBMDk1RDU5QzhFME
                          M4OTVBOUM1ODVFMzQzRTcxNDFD</ds:DigestValue>
                    </ds:Reference>
                  </iodef:HashInformation>
                  <iodef:WindowsRegistryKeysModified>
                    <iodef:Key registryaction="add_value">
                      <iodef:KeyName>
                         HKLM\Software\Microsoft\Windows\
                         CurrentVersion\Run\KB00121600.exe
                      </iodef:KeyName>
                      <iodef:Value>
                         \?\?%AppData%\KB00121600.exe\?\?
                      </iodef:Value>
                    </iodef:Key>
                  </iodef:WindowsRegistryKeysModified>
                </iodef:RecordData>
              </iodef:Record>
            </iodef:EventData>
            <iodef:EventData>
              <iodef:Expectation action="other"/>
                <iodef:Flow>
                  <iodef:System category="source"
                        indicator-set-id="91011">
                    <iodef:Node>
                        <iodef:Address category="url"
                           indicator-uid="qrst">
                              http://foo.com:12345/evil/cc.php
                        </iodef:Address>
                    <iodef:NodeName indicator-uid="rstu">
                        evil.com
                    </iodef:NodeName>
```

```
                    <iodef:Address category="ipv4-addr"
                       indicator-uid="stuv">
                          1.2.3.4</iodef:Address>
                    <iodef:Address category="ipv4-addr"
                       indicator-uid="tuvw">
                          5.6.7.8 </iodef:Address>
                    <iodef:Address category="ipv6-addr"
                       indicator-uid="uvwx">
                           2001:dead:beef::</iodef:Address>
                 <iodef:NodeRole category="c2-server"/>
                 </iodef:Node>
              </iodef:System>
            </iodef:Flow>
            <iodef:Record>
              <iodef:RecordData indicator-set-id="91011">
                <iodef:HashInformation>
                   <ds:Reference>
                      <ds:DigestMethod Algorithm=
                          "http://www.w3.org/2001/04/xmlenc
                           #sha256"/>
                       <ds:DigestValue>
                        141accec23e7e5157de60853cb1e01bc3804
                        2d08f9086040815300b7fe75c184
                       </ds:DigestValue>
                   </ds:Reference>
                 </iodef:HashInformation>
                <iodef:WindowsRegistryKeysModified
                  indicator-set-id="91011">
                  <iodef:Key registryaction="add_key"
                  indicator-uid="vwxy">
                    <iodef:KeyName>
                        HKLM\SYSTEM\CurrentControlSet\
                        Services\.Net CLR
                    </iodef:KeyName>
                  </iodef:Key>
                  <iodef:Key registryaction="add_key"
                    indicator-uid="wxyz">
                    <iodef:KeyName>
                        HKLM\SYSTEM\CurrentControlSet\
                        Services\.Net CLR\Parameters
                    </iodef:KeyName>
                    <iodef:Value>
                        \"\"%AppData%\KB00121600.exe\"\"
                    </iodef:Value>
                  </iodef:Key>
                  <iodef:Key registryaction="add_value"
                    indicator-uid="xyza">
                    <iodef:KeyName>
```

```
                          HKLM\SYSTEM\CurrentControlSet\Services\
                          .Net CLR\Parameters\ServiceDll
                        </iodef:KeyName>
                        <iodef:Value>C:\bad.exe</iodef:Value>
                      </iodef:Key>
                      <iodef:Key registryaction="modify_value"
                        indicator-uid="zabc">
                        <iodef:KeyName>
                            HKLM\SYSTEM\CurrentControlSet\
                            Services\.Net CLR\Parameters\Bar
                        </iodef:KeyName>
                        <iodef:Value>Baz</iodef:Value>
                      </iodef:Key>
                    </iodef:WindowsRegistryKeysModified>
                  </iodef:RecordData>
                </iodef:Record>
              </iodef:EventData>
            </iodef:Incident>
          </iodef:IODEF-Document>
```

A.3. Spear-Phishing

```
<?xml version="1.0" encoding="UTF-8"?>
<IODEF-Document version="1.00" lang="en"
    xmlns="urn:ietf:params:xml:ns:iodef-1.41"
    xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.41"
    xmlns:iodef-sci="urn:ietf:params:xml:ns:iodef-sci-1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <iodef:Incident purpose="reporting">
         <iodef:IncidentID name="csirt.example.com">
            189601
         </iodef:IncidentID>
         <iodef:StartTime>2013-01-04T08:01:34+00:00</iodef:StartTime>
         <iodef:StopTime>2013-01-04T08:31:27+00:00</iodef:StopTime>
         <iodef:DetectTime>2013-01-04T08:06:12+00:00</iodef:DetectTime>
         <iodef:ReportTime>2013-01-04T09:15:45+00:00</iodef:ReportTime>
         <iodef:description>
            Zeus Spear Phishing E-mail with Malware Attachment
         </iodef:description>
            <iodef:Assessment occurrence="potential">
                <iodef:Impact severity="medium" type="info-leak">
                Malware with Command and Control Server and System
                Changes</iodef:Impact>
            </iodef:Assessment>
            <iodef:Contact role="creator" type="organization">
                <iodef:ContactName>example.com CSIRT
```

```
                </iodef:ContactName>
                <iodef:Email>contact@csirt.example.com</iodef:Email>
            </iodef:Contact>
            <iodef:EventData>
              <iodef:Description>Targeting Defense Contractors,
                 specifically board members attending Dummy Con
              </iodef:Description>
            <iodef:Expectation action="other"/>
            <iodef:Method>
               <iodef:Reference indicator_uid="1234">
                  <iodef:ReferenceName>Zeus</iodef:ReferenceName>
                  </iodef:Reference>
            </iodef:Method>
            <iodef:Flow>
               <iodef:System category="source">
                  <iodef:Node>
                    <iodef:Address category="url">
                          http://www.zeusevil.com</iodef:Address>
                    <iodef:Address category="ipv4-addr">
                          10.10.10.166</iodef:Address>
                   <iodef:Address category="as">
                          225</iodef:Address>
                    <iodef:Address category="ext-value"
                      ext-category="as-name">
                      EXAMPLE-AS - University of Example"
                      </iodef:Address>
                    <iodef:Address category="ext-value"
                      ext-category="as-prefix">
                      172.16..0.0/16
                      </iodef:Address>
                    <iodef:NodeRole category="www"
                      attacktype="malware-distribution"/>
                 </iodef:Node>
              </iodef:System>
            </iodef:Flow>
            <iodef:Flow>
               <iodef:System category="source">
                  <iodef:Node>
                   <iodef:NodeName>mail1.evildave.com</iodef:NodeName>
                    <iodef:Address category="ipv4-addr">
                          172.16.55.6</iodef:Address>
                   <iodef:Address category="asn">
                          225</iodef:Address>
                    <iodef:Address category="ext-value"
                      ext-category="as-name">
                      EXAMPLE-AS - University of Example
                     </iodef:Address>
    <iodef:DomainData>
```

```
       <iodef:Name>evildaveexample.com</iodef:Name>
       <iodef:DateDomainWasChecked>2013-01-04T09:10:24+00:00
       </iodef:DateDomainWasChecked>
       <iodef:RelatedDNS RecordType="MX">
           evildaveexample.com MX prefernce = 10, mail exchanger
           = mail1.evildave.com</iodef:RelatedDNS>
       <iodef:RelatedDNS RecordType="A">
           mail1.evildaveexample.com
           internet address = 172.16.55.6</iodef:RelatedDNS>
       <iodef:RelatedDNS RecordType="SPF">
            zuesevil.com. IN TXT \"v=spf1 a mx -all\"
       </iodef:RelatedDNS>
    </iodef:DomainData>
                 <iodef:NodeRole category="mail"
                       attacktype="spear-phishing"/>
                 </iodef:Node>
                 <iodef:Service>
                    <iodef:EmailInfo>
                       <iodef:Email>emaildave@evildaveexample.com
                       </iodef:Email>
                       <iodef:EmailSubject>Join us at Dummy Con
                       </iodef:EmailSubject>
                       <iodef:X-Mailer>StormRider 4.0
                       </iodef:X-Mailer>
                    </iodef:EmailInfo>
                 </iodef:Service>
              </iodef:System>
              <iodef:System category="target">
                 <iodef:Node>
                    <iodef:Address category="ipv4">
                      192.168.54.2</iodef:Address>
                 </iodef:Node>
               </iodef:System>
            </iodef:Flow>

            <iodef:Record>
              <iodef:RecordData>
                <iodef:HashInformation type="file_hash"
                   indicator_uid="1234">
                   <iodef:FileName>Dummy Con Sign Up Sheet.txt
                   </iodef:FileName>
                   <iodef:FileSize>152</iodef:FileSize>
                <ds:Reference>
                   <ds:DigestMethod Algorithm=
                      "http://www.w3.org/2001/04/xmlenc#sha256"/>
                      <ds:DigestValue>
                        141accec23e7e5157de60853cb1e01bc38042d
                        08f9086040815300b7fe75c184
```

```
                    </ds:DigestValue>
                </ds:Reference>
              </iodef:HashInformation>
            </iodef:RecordData>
            <iodef:RecordData>
             <iodef:HashInformation type="PKI_email_ds" valid="0">
               <ds:Signature>
                <ds:KeyInfo>
                   <ds:X509Data>
                      <ds:X509IssuerSerial>
                         <ds:X509IssuerName>FakeCA
                      </ds:X509IssuerName>
                      </ds:X509IssuerSerial>
                      <ds:X509SubjectName>EvilDaveExample
                      </ds:X509SubjectName>
                   </ds:X509Data>
                </ds:KeyInfo>
                   <ds:SignedInfo>
                    <ds:Reference>
                       <ds:DigestMethod Algorithm=
                         "http://www.w3.org/2001/04/xmlenc#sha256"/>
                      <ds:DigestValue>
                       352bddec13e4e5257ee63854cb1f05de48043d09f9
                       076070845307b7ce76c185
                      </ds:DigestValue>
                   </ds:Reference>
                 </ds:SignedInfo>
               </ds:Signature>
             </iodef:HashInformation>
          </iodef:RecordData>
         </iodef:Record>
        </iodef:EventData>
    </iodef:Incident>
</IODEF-Document>
```

Author's Address

Panos Kampanakis
Cisco Systems
170 West Tasman Dr.
San Jose, CA 95134
US

Email: pkampana@cisco.com