# ICSG – Driving Security Standards , Practices and Industry Co-operation

Vincent Weafer, Symantec
Igor Muttik, McAfee

**Industry Connections Security Group**

IEEE
Celebrating 125 Years
of Engineering the Future

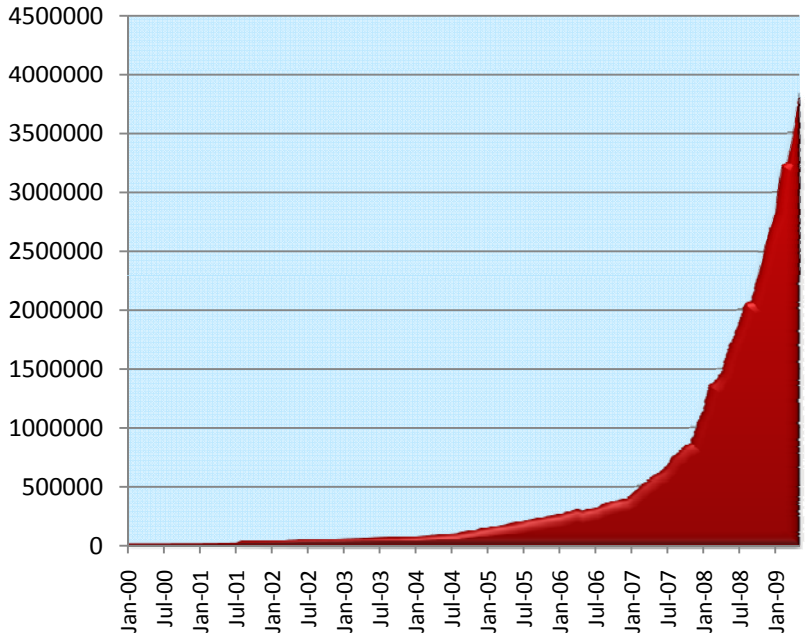
**20th July 2009**

# Agenda

- The problem
- Re-inventing the wheel?
- Introducing ICSG
- Malware Working Group
- XML format
- Main concepts
- Details
- Questions

# The Problem

- Attackers have shifted away from mass distribution of a small number of threats to micro distribution of millions of distinct threats
- The security industry still by and large responds to threats in their individual silo's with 'limited' operational & cross industry co-operation
- The bad actors have been able to leverage the underground economy to gain economies of scale as well as access to specialist tools and services
- Many in the security industry want to pool their experience and resources in response to this systematic and rapid rise in new malware




# Re-Inventing the Wheel ?

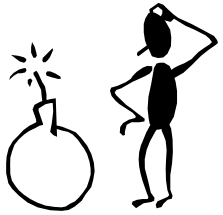
- Lots of great examples of working groups focused on specific aspects of security intelligence , incident response, testing, best practices & policies

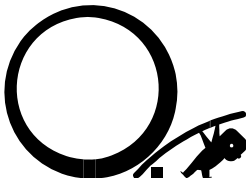
| | |
|---|---|
| ❖APWG | *Anti-Phishing Intelligence & Best Practices* |
| ❖ASC | *Anti-Spyware Intelligence and Best Practices* |
| ❖AMTSO | *Anti-Malware Testing Standards and Best Practices* |
| ❖CARO | *Computer Anti-Virus Research Organization* |
| ❖Others | *AVAR, EICAR, AVPD, MWAAG , FIRST etc* |

# Re-Inventing the Wheel ?

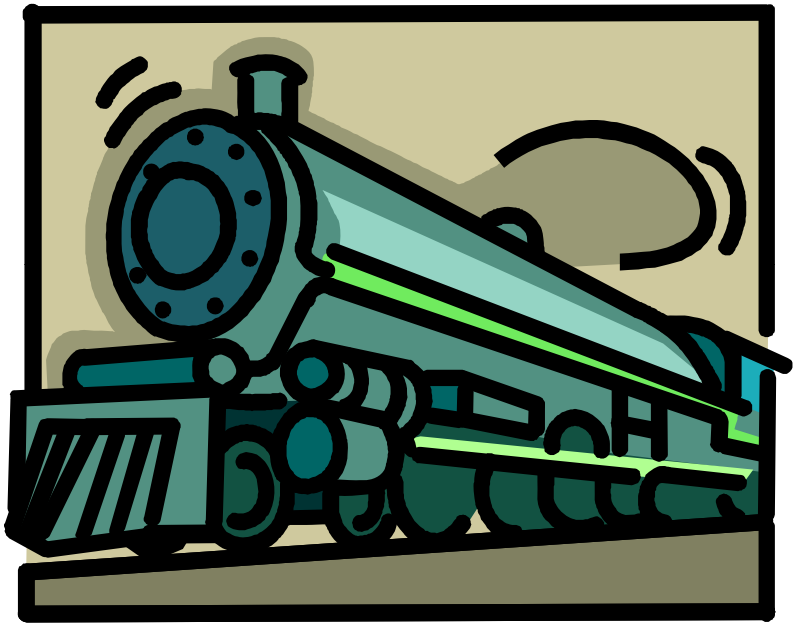
- Lots of great examples of working groups focused on specific aspects of security intelligence , incident response, testing, best practices & policies

*However, this co-operation typically has not been **standardized** or **documented** in a format that lends itself to **systematic improvement** in operational efficiency, or **visibility and review** by people **outside the vertical industries** and in many cases that was not their mandate*





# Introducing



## ICSG

*Industry Connections Security Group*

# ICSG Goal & Structure

- Established under the umbrella of the the IEEE-SA Standards Association
- Facilitate the pooling of industry experience and resources
- Act as a forum for discussions related to the sharing of security protection information and development of proposed standards and best practices
- Membership in ICSG is entity based e.g. corporation, academic institutions, consultancy
- Current executive committee comprised of AVG, McAfee, Microsoft, Sophos, Symantec, Trend Micro, but open to others
- *Goes beyond Malware Issues !*

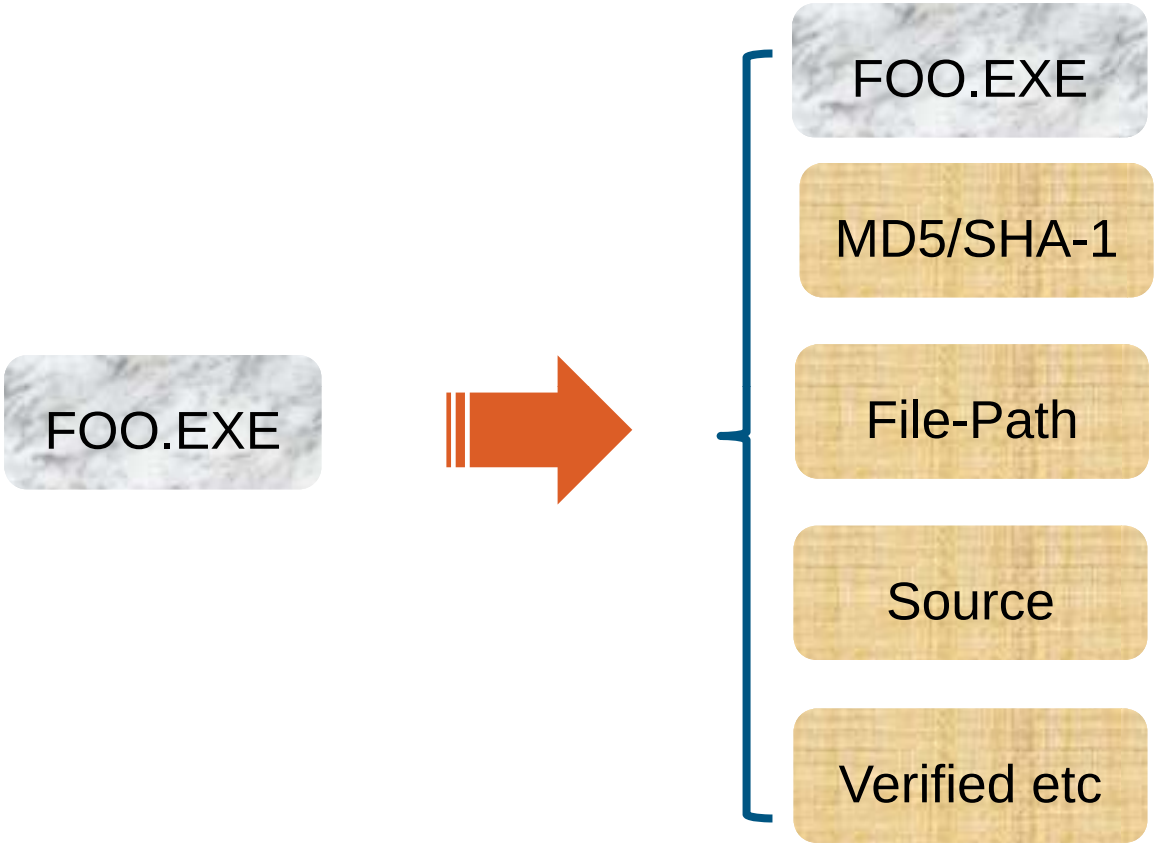
# Why the IEEE?

- Need to reach outside the traditional groups to pool as many different contributors as possible.
- IEEE is a recognized brand known to deliver standards
- The existing infrastructure of the IEEE allowed us to start working on the crux of the issues, instead of wasting time on the org side.
- We leverage the brand to attract the non-traditional players into the pool.

# What to focus on ?

*How do we improve the efficiency of the collection & processing of the millions of malware file samples we all handle each and every month ?*

# How it works




We add available metadata to file sample during transfer (XML format)

# The Benefit

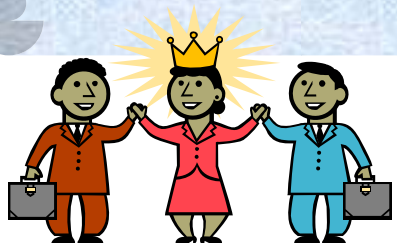
- AV vendors
  - Ability to prioritize sample processing
  - Faster reaction to important threats
  - By their commonality in the field
  - By the “first seen” timestamp
  - Reduces the duplication of samples
- AV testers
  - Helps rank threats
  - Age threats out
  - Run proper “proactive” tests
- Researchers
  - Linking what was hard to link before (e.g. IP ranges, URLs, malware)
  - Persistent knowledgebase in common format
  - More knowledge – more power

# Malware Working Group

- Focused on development of a XML based metadata sharing standard to augment the current industry malware sample sharing process
- Website & Wiki located at http://Ieee.sanasecurity.com
- Home for the schema for validation purposes http://ieee.sanasecurity.com/schema/1.0/metadataSharing.xsd

**Additional Contributors**

*Support Intelligence*
*Immunent*
*Team Cymru*
*ShadowServer*
*Arbor Networks*
*Cisco*
*WebSense*
*AV-Test*
*SonicWall*
*Avira*
*and many others..*



# Development Phases


Initial Design & Feedback ✓

Pilot Deployment

Standardization

Full Deployment

# Key Milestones

| Deliverables | Date |
|---|---|
| Malware Meta-Data Exchange Format (MMDEF) V1 XML Schema document ready for Beta testing by initial WG Participants | 9th April 2009 |
| Final XML Review Meeting by initial WG Participants | 17th April 2009 |
| MMDEF V1 XML Schema document (draft) complete and ready for review with Invitees | 22nd April 2009 |
| MMDEF V1 Review 1 | 1st May 2009 |
| MMDEF V1 Review 2 | 8th May 2009 |
| MMDEF V1 Review 3 | 15th May 2009 |
| MMDEF V1 Review 4 | 22nd May 2009 |
| MMDEF V1 XML Schema document (final) complete and sent for informal WG ballot of readiness for piloting | 29th May 2009 |
| Approval of MMDEF V1 XML Schema document for piloting | 17th June 2009 |
| Piloting of Schema begins | 18th June 2009 |
| TargetPiloting concludes | 31st July 2009 |
| MMDEF V1.1 Schema final edits and review complete (if needed) | August 2009 |
| MMDEF V1.1 Schema balloted | Late August 2009 |

- The next section of the presentation gives a brief outline of the XML schema

# How?

- Outgoing XMLs
  - Along with collection distribution (daily or ad-hoc)
  - RAR-archived (for integrity checking)
  - PGP-encrypted (for authenticated access)
  - Distributed via FTP/SFTP/HTTP/HTTPS
    (same as already used for collection distribution)

- Incoming XMLs will likely be routed into a DB
  - Level of details will depend on the source
  - At least two companies already started distribution

# XML format

- Why XML
  - All is likely to be database-driven – XML is friendly for RDBMS
  - Friendly for humans too
  - Extendable
  - Common and supported everywhere

# Main concepts (1)

- Header
  - Source of meta-data
  - Author
  - Timestamp
- Object1..ObjectNN
  - File
  - URI, domain, service (protocol:port)
  - Environment
  - Registry
  - Entity
- Classification1.. ClassificationMM
  - Clean/dirty/unwanted
  - Malware category
  - Detection name, product, company

# Main concepts (2)

- Relationships1.. RelationshipsXX
  - Child
  - Parent
  - droppedBy, hosts, installed, runs, exploits, downloads, resolvesTo, verifiedBy, usesCNC, contactedBy, operatedByEntity, isnameServerOf, causesToInstall, …
- fieldData1..fieldDataYY
  - firstSeen
  - Origin (e.g. country/collection/honeypot/…)
  - Commonality, priority
- Reference - file[@id="12345"].

# Example (minimal)

```
<?xml version="1.0" encoding="UTF-8"?>
<malwareMetaData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml/metadataSharing.xsd metadataSharing.xsd"
    xmlns="http://xml/metadataSharing.xsd" version="1.0" id="1234">
    <company>McAfee</company>
    <author>Raiden</author>
    <comment>This is minimal - just some files</comment>
    <timeStamp>2008-11-25T21:34:56</timeStamp>
    <objects>
        <!-- files -->
        <file id="2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599">
            <!--<attribute type="filename">116.exe</attribute>-->
            <md5>8b31da6402d850ce94e7c19bc97effe1</md5>
            <sha1>850e5b037c799f86f04ee63da786f9ee139ebf57</sha1>
            <sha256>2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599</sha256>
            <size>32769</size>
            <crc32>34efdbca</crc32>
        </file>
        <file id="3a437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599">
            <!--<attribute type="filename">116.exe</attribute>-->
            <md5>aa31da6402d850ce94e7c19bc97effe1</md5>
            <sha1>990e5b037c799f86f04ee63da786f9ee139ebf57</sha1>
            <sha256>22437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599</sha256>
        </file>
    </objects>
</malwareMetaData>
```

# Example (file+ref+classification)

```
<objects>
    <!-- one file -->
    <file id="2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599">
        <!--<attribute type="filename">116.exe</attribute>-->
        <md5>8b31da6402d850ce94e7c19bc97effe1</md5>
        <sha1>850e5b037c799f86f04ee63da786f9ee139ebf57</sha1>
        <sha256>2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599</sha256>
        <size>32768</size>
    </file>

<!-- one classification -->
    <classification id="AVG:Virut.BK" type="dirty">
        <classificationName>Virut.BK</classificationName>
        <companyName>AVG</companyName>
    </classification>
</objects>


<!-- this file is Virut -->
<relationships>
    <relationship type="isClassifiedAs">
        <parents>
            <ref>file[@id = '2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599']</ref>
        </parents>
        <children>
            <ref>classification[@id='AVG:Virut.BK']</ref>
        </children>
    </relationship>
</relationships>
```

# Example (field data)

```
<!-- this is the prevalence data -->
<fieldData>
    <!-- by file  -->
    <fieldDataEntry>
        <references>
        <ref>file[@id = '2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599']</ref>
        </references>
        <startDate>-1999-11-25T00:00:00</startDate>
        <endDate>2008-11-26T00:00:00 </endDate>
        <origin>user</origin>
        <commonality>8</commonality>
        <location type="countryCodeISO3166-2">US</location>
    </fieldDataEntry>
    <fieldDataEntry>
        <references>
        <ref>file[@id = '2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599']</ref>
        </references>
        <startDate>2008-11-26T00:00:00</startDate>
        <endDate>2008-11-27T00:00:00</endDate>
        <origin>user</origin>
        <commonality>5</commonality>
        <location type="countryCodeISO3166-2">US</location>
    </fieldDataEntry>
    <fieldDataEntry>
        <references>
        <ref>file[@id = '2f437c1c8f73c2d6ffbb6214d3f1ccfe994151b3bd80fe2b3934a1bc89384599']</ref>
        </references>
        <startDate>2008-11-27T00:00:00</startDate>
        <endDate>2008-11-28T00:00:00</endDate>
        <origin>user</origin>
        <commonality>1</commonality>
    </fieldDataEntry>
```

# Next Steps

- We’re looking for active members of the Malware Working Group
- We need more participants in the pilot
- We need ideas on critical areas we should focus on
  - Ideas so far include blacklisting of malicious & predominately malicious packers/obfuscators .

# Questions