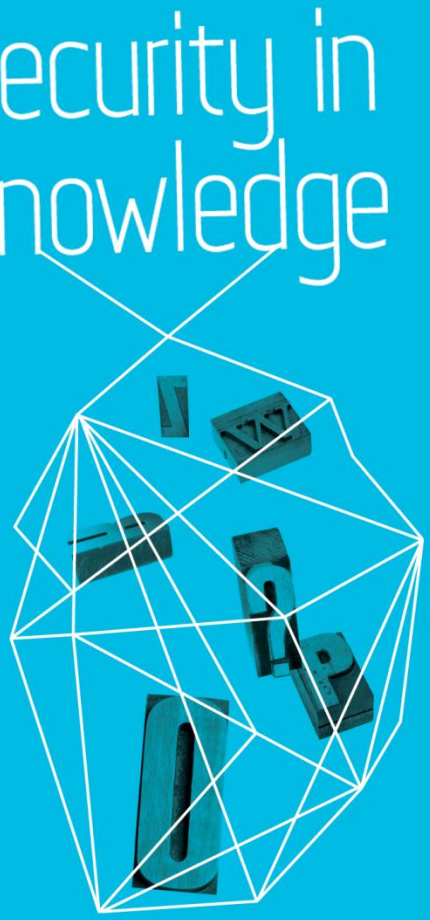
# Sharing Indicators of Compromise: An Overview of Standards and Formats




Chris Harrington
EMC Critical Incident Response Center

Session ID: DSP-W25A
Session Classification: Intermediate

# Indicator of Compromise (IoC)?

- A piece of information that can be used to search for or identify potentially compromised systems.

- Examples
  - IP Address / Domain Name
  - URL
  - File Hash
  - Email Address
  - X-Mailer
  - HTTP User Agent
  - File Mutex

# Why do we want to share IoCs?

- Faster access to actionable security information, often peer / industry relevant
- Causes the threat actors to change infrastructure more frequently
- Builds trust relationships between organizations
- Supports an Intelligence Driven security model

# Problem Statement

- There is currently no generally accepted standard data format for Security teams to share Indicators of Compromise (IoCs)
  - Causes the sharing and processing of IoCs to be a manual process which impacts participation
    - Who likes copying and pasting from forums / portals?
  - Vendor adoption of any standard extremely limited.
    - VHS vs. Beta?

# OpenIOC

- Open Indicators Of Compromise
- Source: Mandiant

- “OpenIOC is an extensible XML schema for the description of technical characteristics that identify a known threat, an attacker’s methodology, or other evidence of compromise.”

- http://www.openioc.org/

# OpenIOC

- Pros
  - Free (Apache 2 license)
  - Extensible, can be extended as needed
  - Free IOC Editor software to create OpenIOC indicators
  - Full support in Mandiant products
- Cons
  - Limited commercial adoption (outside of Mandiant)
  - Limited Network based IoC support
    - Generic Network String needed to cover many IoCs
  - Viewed as a “vendor” solution
  - No support for describing Tactics, Techniques, and Procedures

# CybOX

- Cyber Observable eXpression
- Source: MITRE

- “the Cyber Observable eXpression (CybOX) is a standardized schema for the specification, capture, characterization and communication of events or stateful properties that are observable in the operational domain.”

- http://cybox.mitre.org/

# CybOX

- Pros
  - Very comprehensive list of elements to build IoCs
  - Support for “free text” and comments
  - Integration with CAPEC & MAEC under STIX for robust IoCs
  - Vendor neutral in origin
- Cons
  - Limited commercial adoption
  - Requires other formats to describe TTPs or campaigns
  - Fairly large schema

# IODEF

- Incident Object Description Exchange Format
- IETF Standard (RFC 5070)
  - Combined with RFC 5901 (Phishing) for IoC usage

- “The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.”

- www.ietf.org/rfc/rfc5070.txt

# IODEF

- Pros
  - Open Standard through IETF
  - Vendor neutral in origin
  - Commercial adoption (ArcSight)
- Cons
  - Limited native IoC descriptive capability
    - Requires RFC 5901 and / or extensions
  - Requires other formats to describe TTPs or campaigns
  - Designed to share Incident data, not IoCs
  - Dated (last updated in 2007) but being update as we speak

# Which is best?

- Depends
- Each has plus / minus
- Specific need will drive your adoption, unless you are relying on vendor implementation

**None of these meet 100% of my needs**

# Overall Limitations

- Limited ability to describe Attribution or Relationship
  - First thing asked when sharing an IoC is “what threat actor or campaign is this tied to?”
- Limited support for additional details
  - An IP address isn’t an IoC (it isn’t a good one anyway)
    - Is it a C2 or Malware delivery site?
    - Is it a legit site that was compromised or a rogue site?
- Host based IoC focus
  - Support for Network IoCs is generally much less
    - i.e. HTTP User Agent or X-Mailer

# Current Improvement Initiatives

- MILE Working Group
  - Charter is to review IODEF and make necessary changes to reflect today's threats.
- Structured Threat Information eXpression (STIX)
  - "…collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information."
- Trusted Automated eXchange of Indicator Information (TAXII)
  - "…is a set of technical specifications and supporting documentation that enable organizations to exchange cyber threat information in a secure, automated manner."

# Questions?

# Thank You