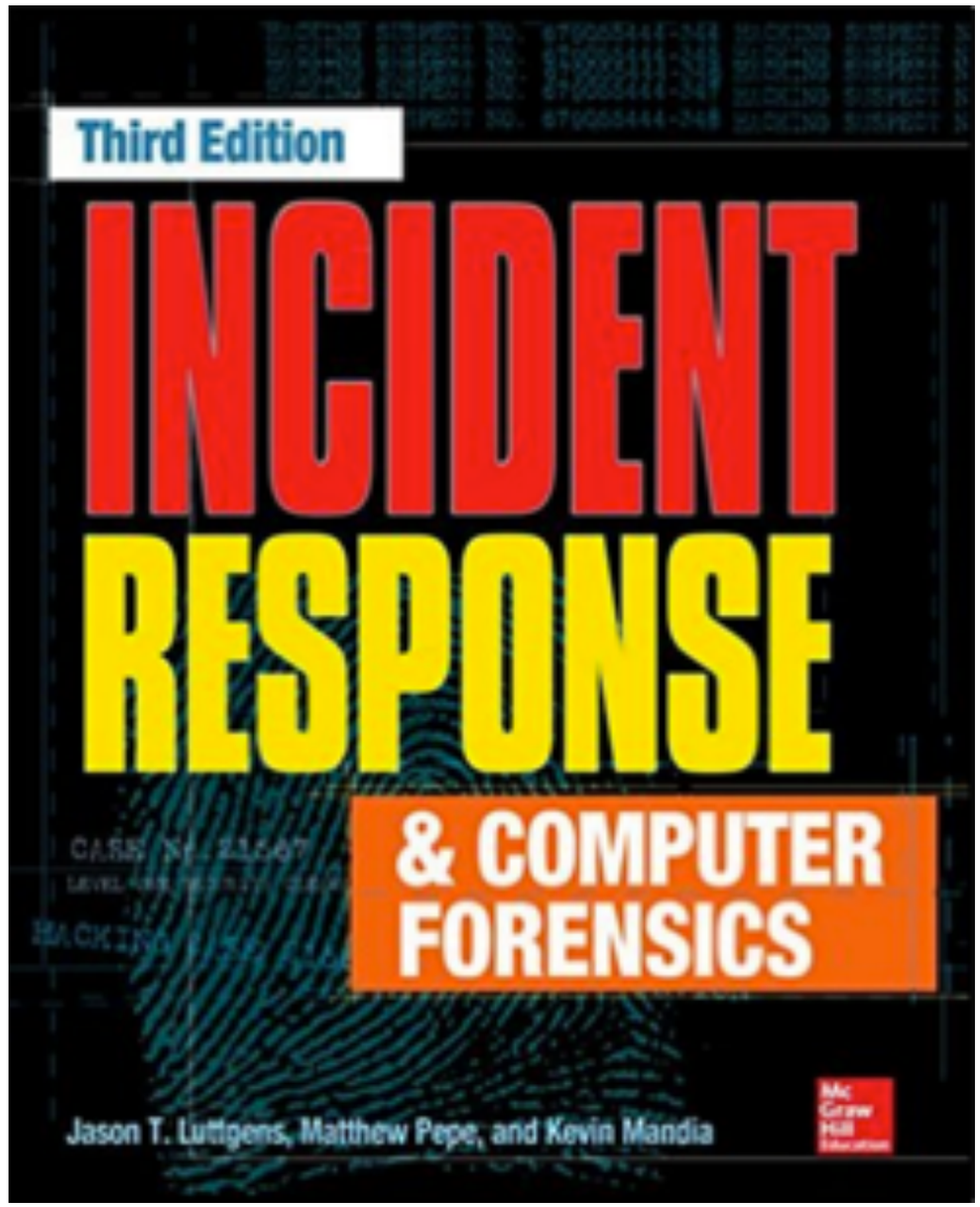
CNIT 121: Computer Forensics



2 IR Management Handbook

What is a Computer Security Incident?

- Intent to cause harm
- Was performed by a person
- Involves a computing resource

Examples

- Data theft, including sensitive personal information, e-mail, and documents
- Theft of funds, including bank access, credit card, and wire fraud
- Extortion
- Unauthorized access to computing resources
- Presence of malware, including remote access tools and spyware
- Possession of illegal or unauthorized materials

Goals of IR

- Investigate
  - Determine the initial attack vector
  - Determine malware and tools used
  - Determine what systems were affected, and how
  - Determine what the attacker accomplished (damage assessment)
  - Determine if the incident is ongoing
  - Establish the time frame of the incident
- Remediate
  - Using the information obtained from the investigation, develop and implement a remediation plan

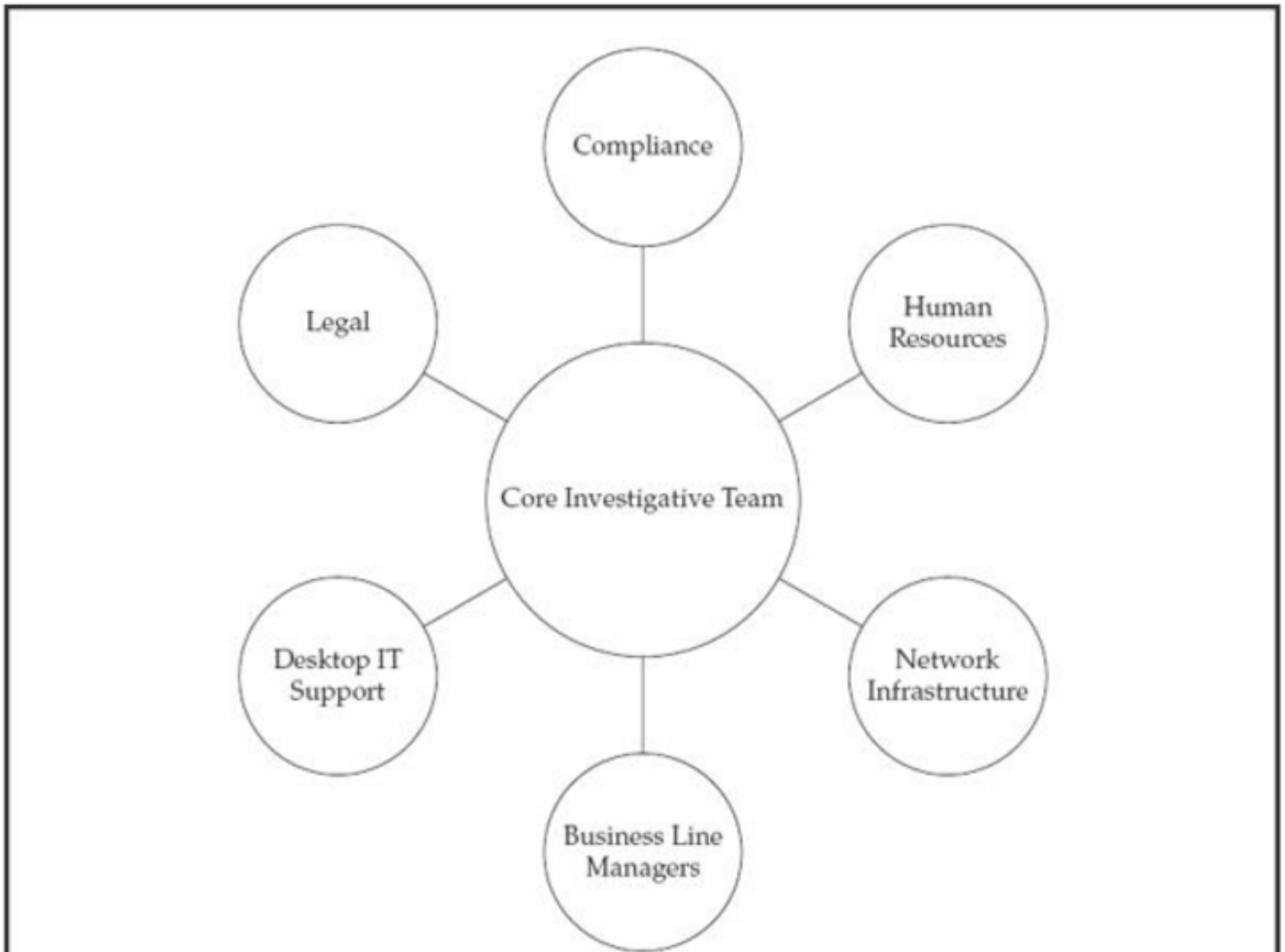


Figure 2-1. Team composition

Incident Manager

- **Leads the investigation team**
- **Must be able to get information and request actions quickly**
- **Often the CIO, CISO, or someone they directly appoint to work on their behalf**

Remediation Team Leader

- **Experienced member of IT staff**
- **Focal point for all remediation activities, including**
  - **Corrective action**
  - **Evaluating the sensitivity of stolen data**
  - **Strategic changes that will improve the orgqaniations security posture**

Ancillary Teams

- Representatives from internal and external counsel
- Industry compliance officers (for example, PCI, HIPAA, FISMA, and NERC)
- Desktop and server IT support team members
- Network infrastructure team members
- Business line managers
- Human resource representatives
- Public relations staff

PCI-DSS

One industry that is notorious for imposing processes and standards on investigations is the Payment Card Industry. Once the card brands get involved in your investigation, your recovery is secondary to their goals of protecting their brands and motivating your organization to be PCI DSS compliant.

Finding IR Talent

- **Cost of maintaining an IR team**
- **Culture of outsourcing**
- **Mandated by regulatory or certification authorities**
- **Inexperience in investigations**
- **Lack of or limited in-house specialization**

How to Hire IR Talent

- **Finding candidates**
  - **Already working on other IR teams**
  - **Online IR social networking sites**
  - **College programs in computer science, engineering, or computer forensics**
    - **Preferably post-graduate**

How to Hire IR Talent

- **Assessing the Proper Fit: Capabilities and Qualities**
  - **Experience in running investigations involving technology**
  - **Experience in performing computer forensics examinations**
  - **Experience in network traffic analysis**
  - **Knowledge of applications relevant to your organization**

IR Team Member Characteristics

- Highly analytical
- Good communicator
- Attention to detail
- A structured and organized approach to problem solving
- Demonstrable success in problem solving

Industry Certifications

- **Certs requiring periodic retesting and demonstration of continuing education**

- **Too many certs indicate shallowness**

The Incident Response Process

Three Main Activities

- Initial response
- Investigation
- Remediation

Initial Response

- **Assemble the response team**
- **Review network-based and other readily-available data**
- **Determine type of incident**
- **Assess potential impact**

Common Tasks

- Interview the person(s) who reported the incident. Gather all the relevant details they can provide.
- Interview IT staff who might have insight into the technical details of an incident.
- Interview business unit personnel who might have insight into business events that may provide a context for the incident.
- Review network and security logs to identify data that would support that an incident has occurred.
- Document all information collected from your sources.

Investigation

- **Goal is to determine**
  - **What happened**
  - **How it happened**
  - **Sometimes, who was responsible**
- **Simply re-imaging servers without this knowledge is uncertain and risky**

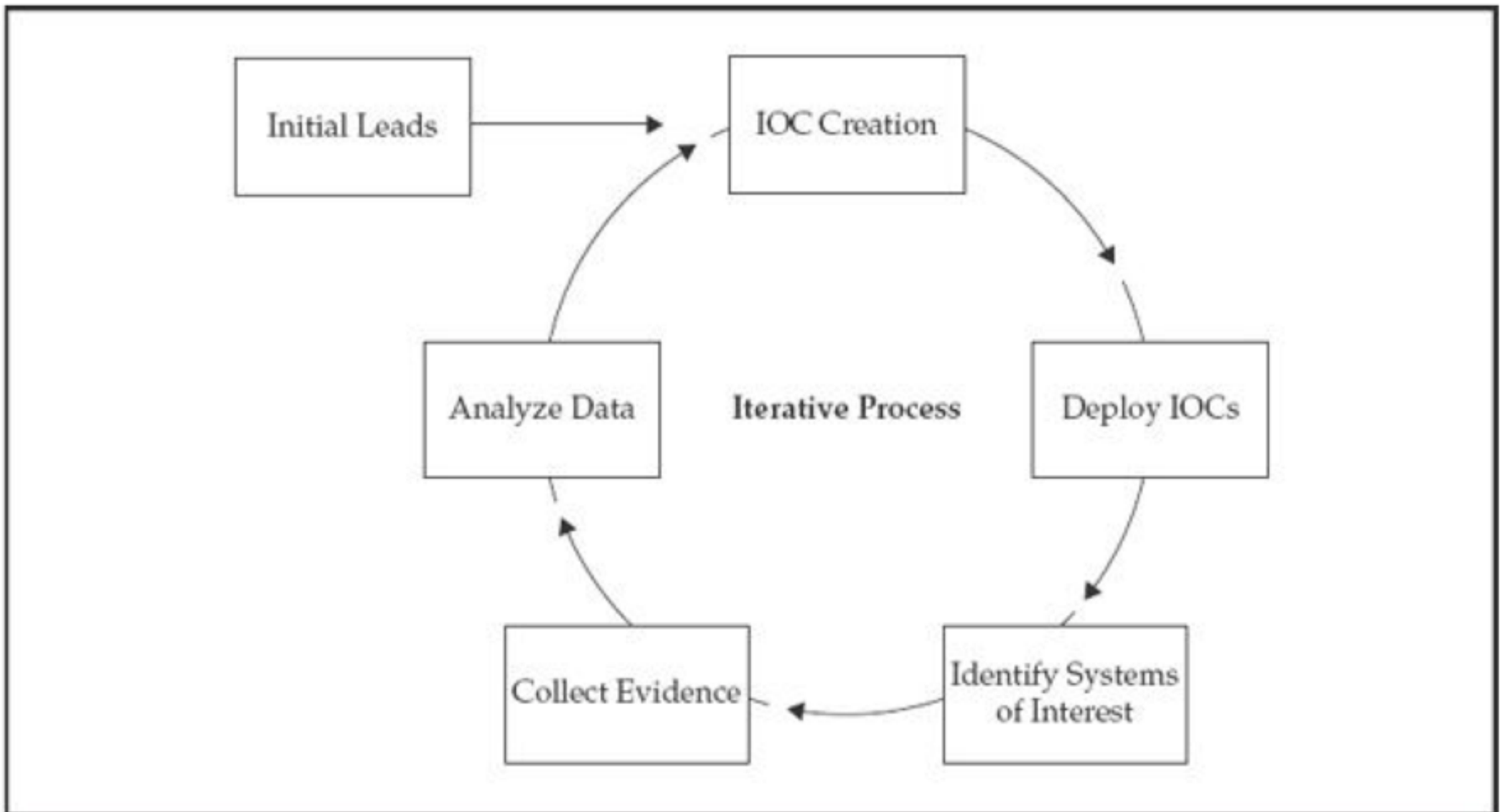


Figure 2-2. The incident response lifecycle

Don't Act too Quickly

- **Jumping into remediation without all the facts is risky**
- **Attacker may detect your remediation and dig in deeper**
- **Usually better to gather more complete information to plan a more complete remediation action**

Initial Leads

- **Don't focus exclusively on malware**
- **Once attacker has a foothold and gathers credentials, he no longer needs malware**
- **Good leads are**
  - **Relevant to current incident**
  - **Detailed -- with IP addresses, date & time, etc.**
  - **Actionable - you have logs that can be followed**

Indicators of Compromise (IOC) Creation

- **Working directory names**
- **Output file names**
- **Login events**
- **Persistence mechanisms**
- **IP addresses**
- **Domain names**
- **Malware network protocol signatures**

IOC Formats

- Mandiant's OpenIOC (www.openioc.org)
- Mitre's CybOX (cybox.mitre.org)
- YARA (code.google.com/p/yara-project)

Example IOC

openioc.org/iocs/c32ab7b5-49c8-40cc-8a12-ef5c3ba91311.ioc

```
▼<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns="http://schemas.mandiant.com/2010/ioc" id="c32ab7b5-49c8-40cc-8a12-ef5c3ba91311" last-modified="2011-10-28T19:28:20">
   <short_description>FIND WINDOWS</short_description>
  ▼<description>
     This is a sample IOC that will hit on a number different artifacts present on a Windows computer. This IOC is used to test or
     illustrate the use of an IOC.
   </description>
   <keywords/>
   <authored_by>Mandiant</authored_by>
   <authored_date>0001-01-01T00:00:00</authored_date>
   <links/>
  ▼<definition>
   ▼<Indicator operator="OR" id="2e693207-ae90-4f9b-8a31-67f31f1d263c">
    ▼<IndicatorItem id="5ebfad1c-6f1a-472b-ae58-6fdfede0f4e7" condition="contains">
       <Context document="FileItem" search="FileItem/FullPath" type="mir"/>
       <Content type="string">\kernel32.dll</Content>
     </IndicatorItem>
   ▼<IndicatorItem id="5b79c908-9d4d-4536-8699-9538af1576e8" condition="is">
       <Context document="FileItem" search="FileItem/FileName" type="mir"/>
       <Content type="string">win.ini</Content>
     </IndicatorItem>
   ▼<IndicatorItem id="d1e188e1-fae6-488d-ba2f-a900abb21f14" condition="contains">
       <Context document="FileItem" search="FileItem/FileExtension" type="mir"/>
       <Content type="string">evt</Content>
     </IndicatorItem>
   ▼<IndicatorItem id="78af913e-a007-4f8a-864f-b543dd7a6d09" condition="is">
       <Context document="ProcessItem" search="ProcessItem/name" type="mir"/>
       <Content type="string">explorer.exe</Content>
     </IndicatorItem>
```

- **Link Ch 2a**

IOC Deployment

- **Find compromises in an automated fashion with**
  - **Enterprise IR platform**
  - **Visual Basic scripts**
  - **Windows Management Instrumentation (WMI) scripts**

IOC Formats

- **For network signatures, Snort rules are the standard**

- **There are three IPC formats, but none has emerged as the clear leader and an industry standard yet**

Identify Systems of Interest

- **After deploying IOCs, you find "Hits"**
  - **A match for a rule or IOC**
- **Review matching information to see if the hit is valid**
- **Hits can be false positives**

Initial Triage

- **Validate**
  - **Check time frame and other data to make sure the matching item is relevant**
- **Categorize**
  - **Assign systems to meaningful categories like "Backdoor installed", "Access with valid credentials", "SQL injection", "Credential harvesting", or "Data theft"**
- **Prioritize**
  - **Highest priority given to machines that offer new investigative leads, such as a different backdoor**

Preserve Evidence

- **Minimize changes to a system**
- **Minimize interaction time with a system**
- **Create appropriate documentation**
- **Can collect evidence from a running system or take it down for imaging**
- **Don't collect large volumes of data that may never be examined**

Evidence Preservation Categories

- **Live response**
  - **Most common method**
    - **Use an automated tool to collect standard data from a running system**
    - **Contains volatile and nonvolatile information**
      - **Process list, active network connections, event logs, a list of objects in the file system, registry**
      - **Contents of log files and suspected malware**

Evidence Preservation Categories

- **Memory collection**
  - **Most useful when the attacker is hiding activities, such as a rootkit, and you cannot obtain a disk image**
  - **Useful for memory-resident malicious activity**
  - **Not worth the bother on most systems, because there's not enough data to answer high-level questions**
  - **No way to explain how malware got there, or what the attacker has been doing**

Evidence Preservation Categories

- **Forensic Disk Image**
  - **Complete duplicate of a hard disk**
  - **Images are large and take a long time to analyze**
  - **Only worth it if necessary; such as when the attacker performed many actions over a long time, or where information is required that can't be found elsewhere**
  - **If no intrusion is suspected, a disk image is the norm**

Analyze Data

- **Malware analysis**
- **Live response analysis**
- **Forensic examination (on disk images)**
  - **Make a list of realistic questions to answer**
  - **Don't allow time to be wasted here**

Remediation

- **Remediate when detection methods stop finding new events ("steady state")**
- **Start planning remediation early in the IR process**
- **There are many moving parts to any organization**
- **Coordinating threat removal is not an easy task**

Three Activities

- Posturing
- Tactical (short term)
- Strategic (long term)

Posturing

- **Steps that ensure the success of remediation**
  - **Establishing protocol**
  - **Exchanging contact information**
  - **Designating responsibilities**
  - **Increasing resources**
  - **Scheduling resources and coordinating timelines**

Tactical

- **Actions to address the current incident**
  - **Rebuilding compromised systems**
  - **Changing passwords**
  - **Blocking IP addresses**
  - **Informing customers**
  - **Making internal or public announcement**
  - **Changing a business process**

Strategic

- **Long-term improvements**
- **May require significant changes within an organization**

Tracking Significant Investigative Information

- **Track critical information**
- **And share it with ancillary teams and organization's leadership**
- **Incident numbering or naming system**

Significant Investigative Information

- **List of evidence collected**
  - **With date, time, source, and chain of custody**
- **List of affected systems**
- **List of files of interest**
- **List of accessed or stolen data**

Significant Investigative Information

- **List of significant attacker activity**
- **List of network-based IOCs**
- **List of host-based IOCs**
- **List of compromised accounts**
- **List of ongoing and requested tasks for your teams**

Reporting

- **Reports are fundamental deliverables for consultants**

- **Periodic, formal report keep track of all the finding and keep the investigation focused**

- **Writing the report helps you organize your activities**