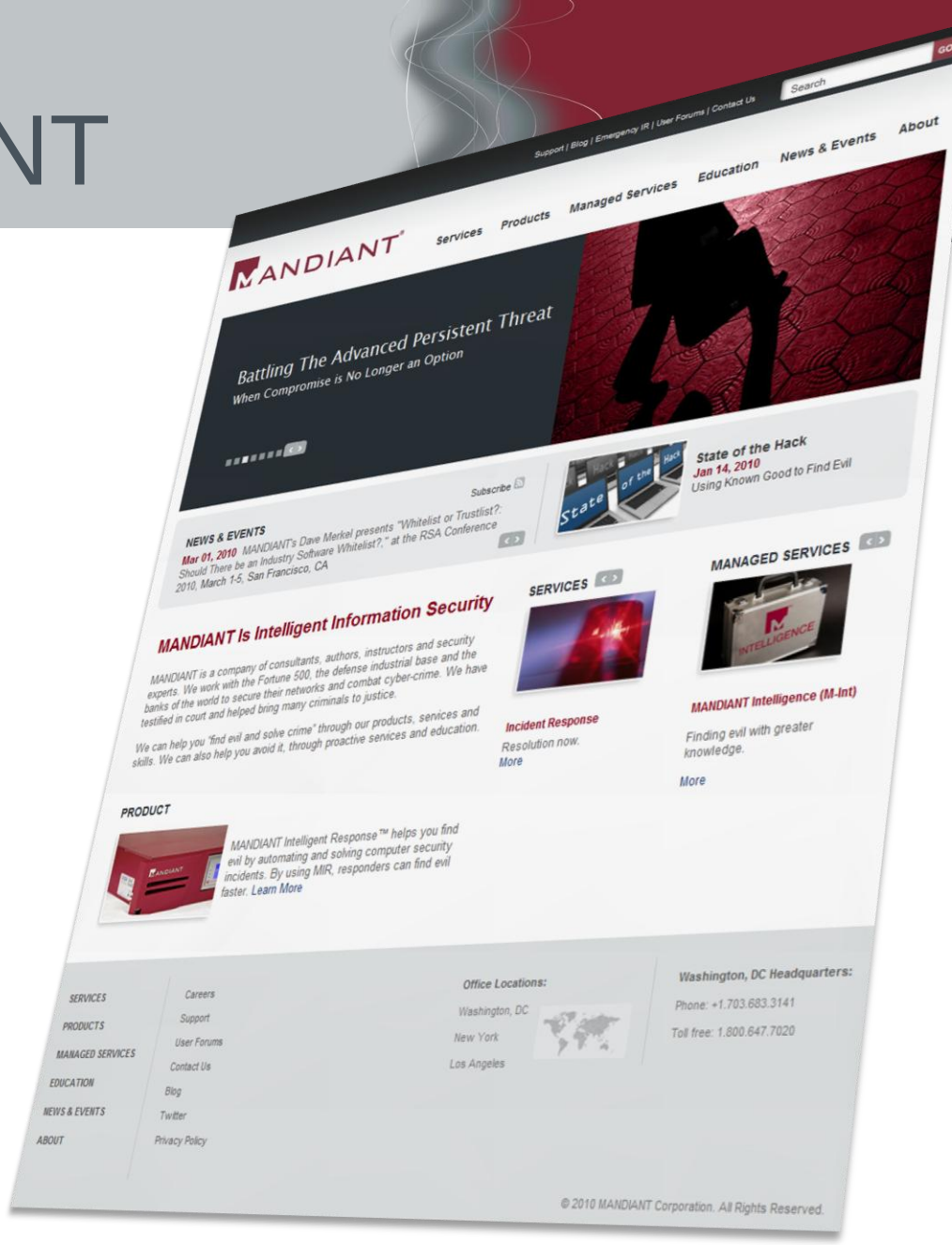
SwA Forum 2011: APT Panel

Ryan Kazanciyan, Principal Consultant
ryan.kazanciyan@mandiant.com

We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- APT & CDT experts
- Application and Network Security Evaluations
- Located in
  - Washington
  - New York
  - Los Angeles
  - San Francisco
- Professional and managed services, software and education



whoami

MANDIANT

RYAN KAZANCIYAN

[kah-ZAN-see-yan]

- Principal Consultant
- Incident response, forensics, penetration testing, application security
- Instructor for BlackHat, LE courses
- > 13 APT investigations in the past year

“State of the Hack” APT Intrusions

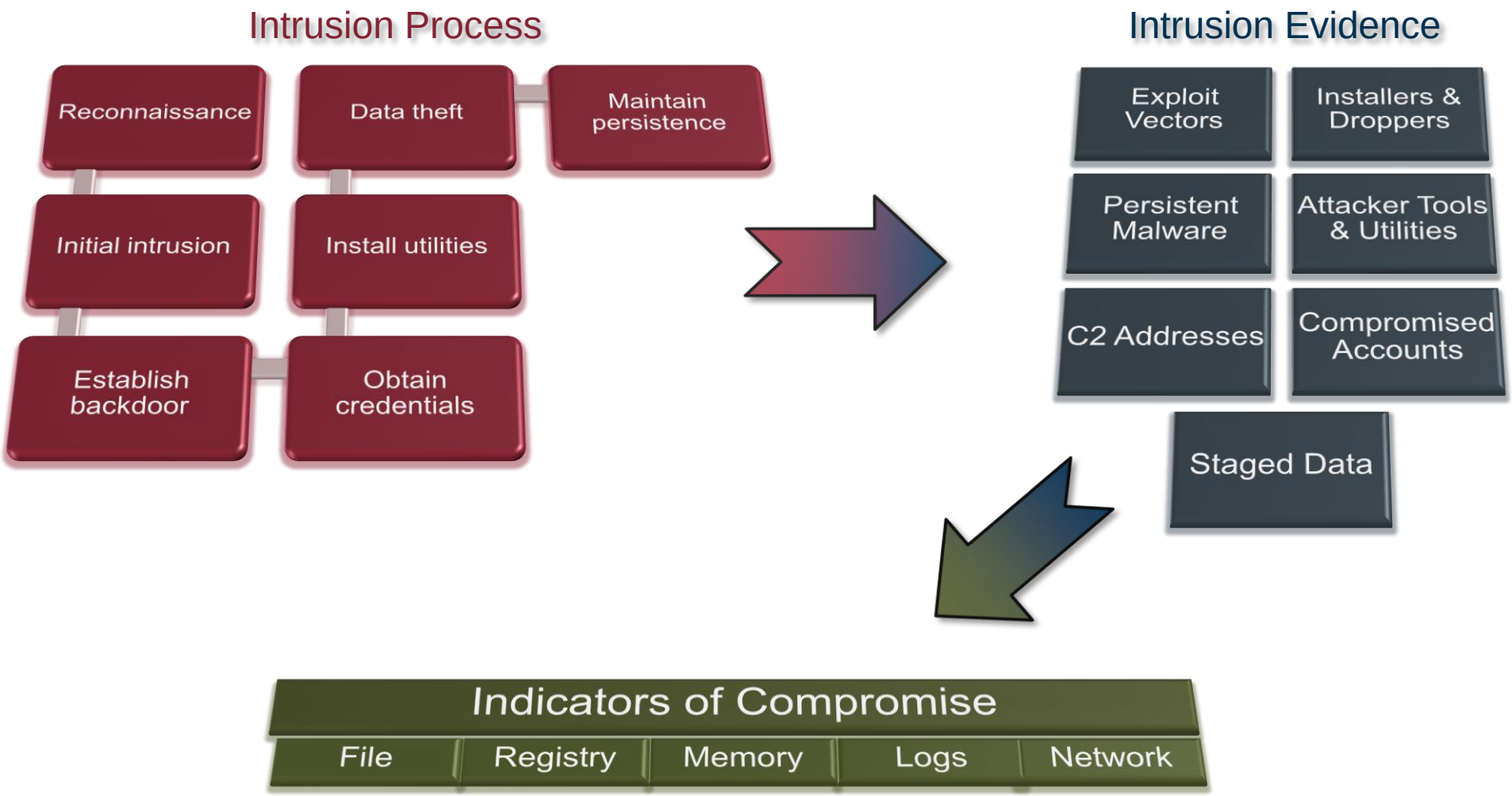
- ***Who*: Well-equipped adversaries with specific collection objectives**

- ***How*: Exploitation, persistence, data theft remain trivial**
  - “Perimeter” (Layer 8 - users) insecurity
  - Internal network insecurity
  - Unreliable preventative controls

Investigative Challenges

- ***Limited knowledge*** from initial breach detection (or notification)
- ***Fully scoping*** the compromise before remediation
- Conducting ***enterprise scale*** host and network-based forensic analysis
- ***Rapid detection, containment, and response*** is the new prevention

From intrusion to IOCs

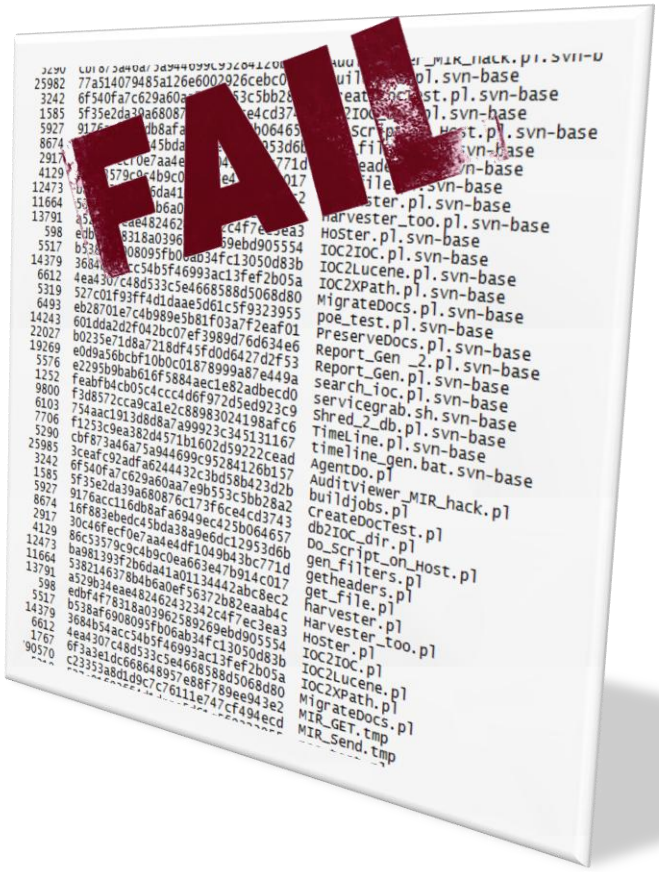


The OpenIOC Format

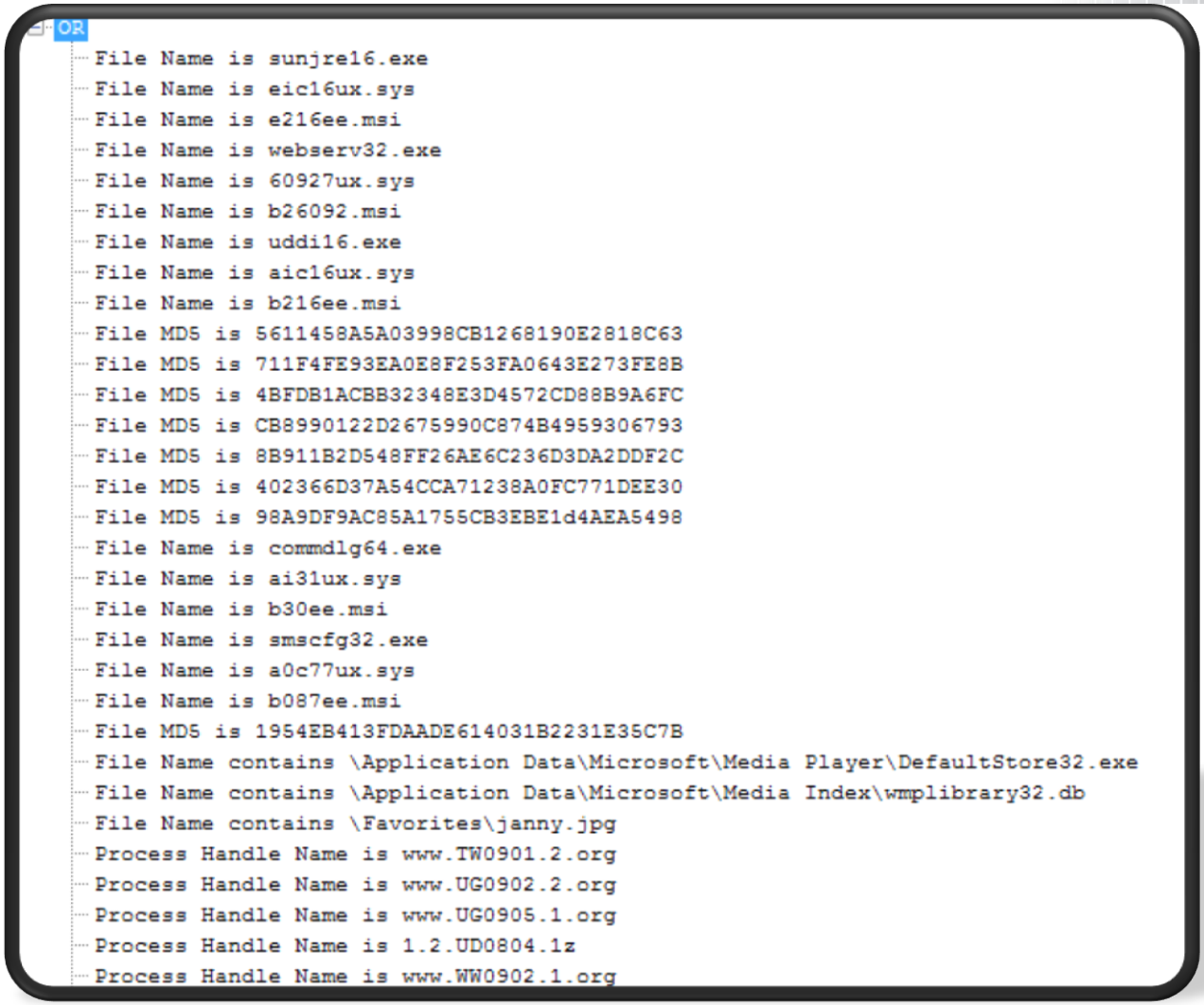
- IOC = “Indicator of Compromise”
- A format to organize your intelligence
- Logical groupings of forensic artifacts
- Extendable for any indicator type
- XML (of course)
- Based on lessons learned in the field

Before OpenIOC

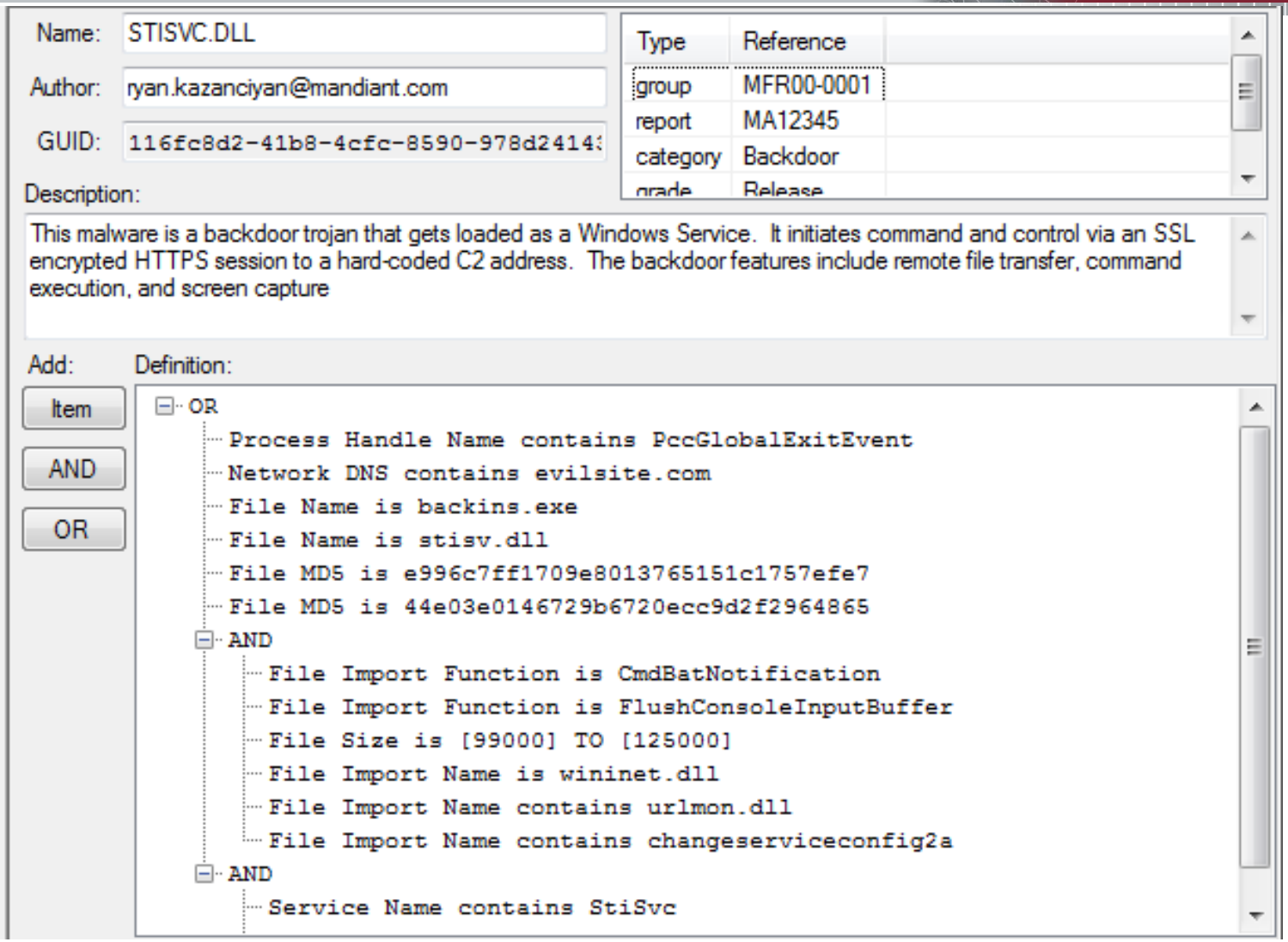
- Lists of stuff to find evil
  - Easy to create
  - Difficult to maintain
  - Terrible to share
- Lists do not provide context
  - An MD5 of what?
  - Who gave me this?
  - Where is the report?
  - Where is the intelligence??
- **Lists encourage reliance on easily mutable forensic artifacts**



IOC allows this…



…to become this



Our IOC schema

- 37 IOC characteristics shown (out of our current 233)
- OpenIOC schema easily edited and expanded

Characteristics	Definition of Characteristic
File Accessed Time	Last access time of a file
File Attribute	Attributes of a file (Read-only, Hidden, System Directory, etc.)
File Changed Time	File name modified of a file
File Compile Time	Checks the compile time of a file
File Created Time	Creation time of a file
File Digital Signature Description	Description of whether the signature is verified or not
File Digital Signature Exists	Verifies that a digital signature exists
File Digital Signature Verified	Verifies a digital signature is valid
File Export Function	Export function declared by a file
File Extension	Extension of a file
File Full Path	Full path for a file
File Import Function	Import function declared by a file
File Import Name	Import name declared by a file
File MD5	MD5 of the file
File Modified Time	Modified time of a file
File Name	Name of a file
File Owner	Owner of the file
File Path	Path of a file
File PE Type	Checks the PE type of a file

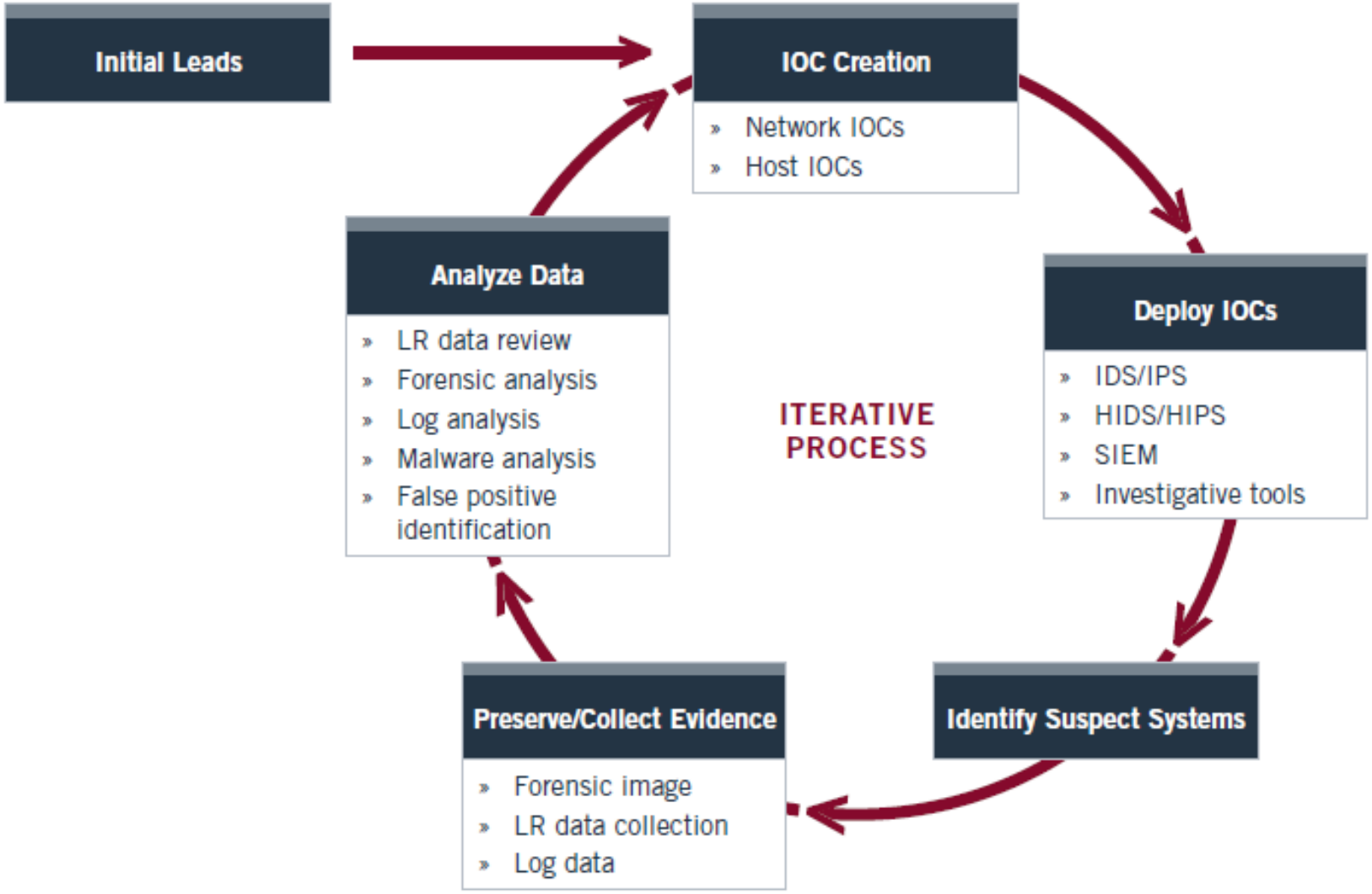
Characteristics	Definition of Characteristic
File PeakEntropy	Peak entropy of a file
File Raw Checksum	Calculated checksum of a file
File Size	Size of the file
File Strings	Readable strings of a file's binary data
Network DNS	DNS queries on a network
Network String URI	URI associated with network traffic
Network String User Agent	User agent associated with network traffic
Process Handle Name	Name of a process handle
Process Name	Name of a process
Registry Key ModDate	Modification time of a registry key
Registry NumSubKeys	Checks the total number of subkeys associated to a registry key
Registry Path	Path of a registry item
Registry Text	Contents of the registry text field
Service Descriptive Name	Description text of a service
Service DLL	DLL implemented by a service
Service Name	Name of a Service
Service Path	Path to the service file
Service Status	Checks the current status of a service

Types of IOCs

MANDIANT

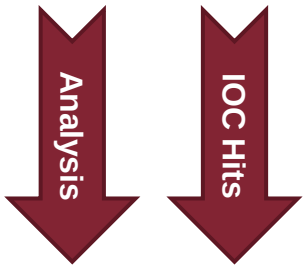
Signature	Generic	Methodology
• Specific & targeted • MD5, compile time, file size, file name + path, etc.	• Characteristics unique to a family of variants • Rack & stack data (e.g. services)	• Focus on what attacker *does* rather than what malware *is* • Staging locations, name conventions, etc.

Using IOCs in the investigative lifecycle

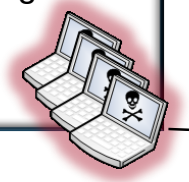


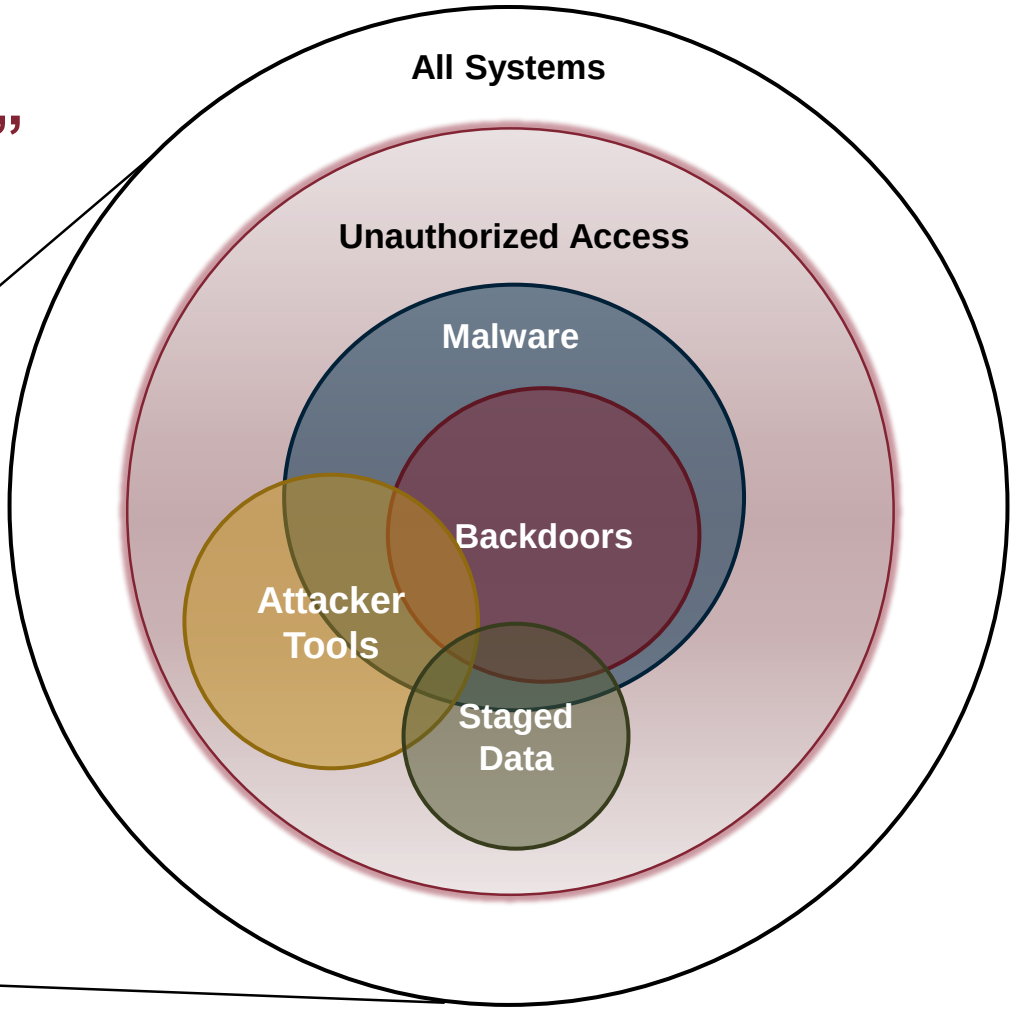
Scoping the incident

What is a "compromised" system?



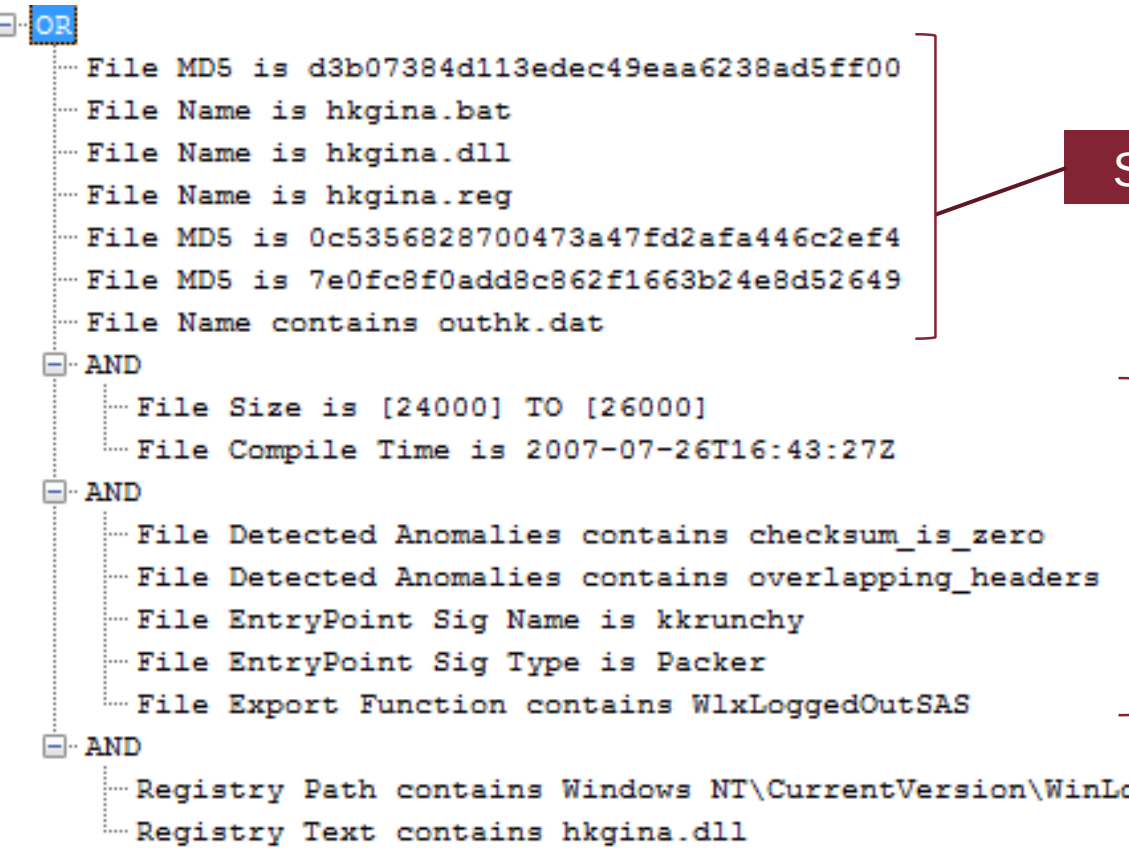
- Backdoored systems
- Systems with malware
- Accessed systems
- Systems with staged data
- Compromised credentials





IOC Examples

Signature + Generic IOC



Specific

Generic

Specific

Malware Analysis Report

...This malware is a "GINA" (Graphical Identification and Authentication) replacement. It records all users who log on to the system and their passwords to file "outhk.dat"...

Generic IOCs: Services

Known Services (excerpts)

```
AND
    Service Name is themes
    Service DLL contains not \system32\shsvcs.dll
    Service DLL contains not \system32\themeservice.dll
AND
    Service Name is shellhwdetection
    Service DLL contains not \system32\shsvcs.dll
AND
    Service Name is lanmanserver
    Service DLL contains not \system32\srvsvc.dll
```

Whitelist by ServiceDLL name

Whitelist by service Digital Signatures

```
AND
    Service Name is lanmanserver
    ServiceItem/serviceDLLSignatureVerified is false
AND
    Service Name is termservice
    ServiceItem/serviceDLLSignatureVerified is false
    Service Path Signature Verified is false
AND
    Service Name is trkwks
    ServiceItem/serviceDLLSignatureVerified is false
AND
```

Generic IOCs & Stacking: Process User “services.exe”

MANDIANT

Path	Username	Count
d:\documents and settings*\local settings\application data	**XXXX\e343141**	**1**
d:\documents and settings\local settings\application data**	**XXXXX\e419461**	**1**
d:\documents and settings*\local settings\application data**	**XXXXXX\e439074**	**1**
c:\windows\system32	nt-hallinta\system	3
c:\windows\system32	nt-myndighet\system	5
c:\windows\system32	zarzadzanie nt\system	22
c:\windows\system32	nt instans\system	33
c:\windows\system32	nt-autorität\system	137
c:\windows\system32	autorite nt\system	531
c:\windows\system32	nt authority\system	12752

Methodology IOCs

```
OR
  AND
    File Name is index.dat
    File Strings contains System Volume Information
  AND
    File Name contains hh.dat
    File Strings contains 2011 Salary.chm
  URL History URL contains www.innocuous-site.org
  EventLog user contains ADOMAIN\User12
  File Owner is ADOMAIN\User12
```

Activity-based:
- Files opened
- CHM file opened
- Website visited

Compromised User:
- Events generated
- Files owned

Evidence of suspicious scheduled tasks

```
OR
  AND
    OR
      File Full Path contains \Windows\SchedLgU.txt
      File Full Path contains \Winnt\SchedLgU.txt
    OR
      File Strings contains at1.job
      File Strings contains at2.job
      File Strings contains cmd.exe
      File Strings contains at3.job
      File Strings contains at4.job
      File Strings contains at5.job
```

Conclusion

Don’t Panic!

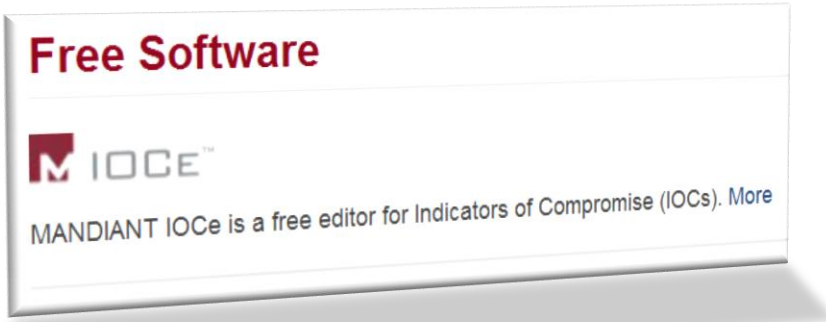
- Avoid knee-jerk responses to detected breaches
- You probably only know a small piece of a larger puzzle
  - Compromised systems
  - Accessed systems
  - Malware and utilities in place
  - Malicious network endpoints
- Incomplete response ensures attacker adaptation and persistence

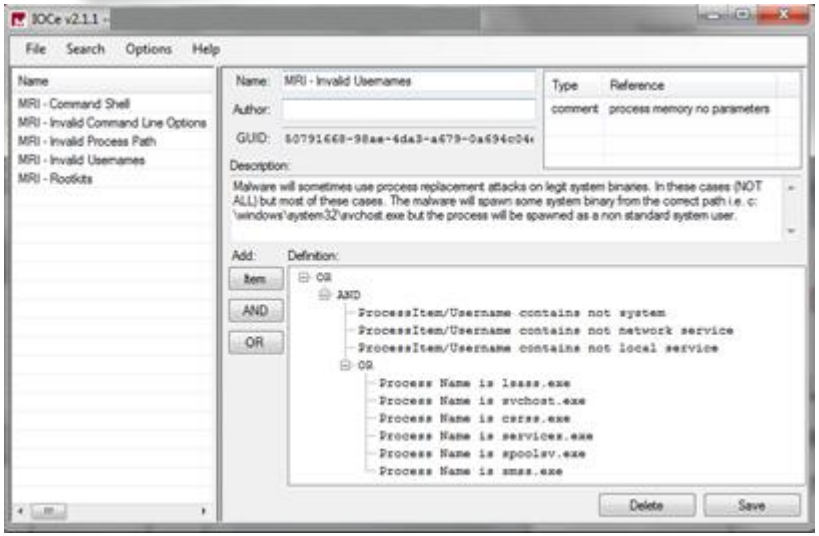
Free resources

- Free tools
  - IOCe
  - Memoryze
  - Audit Viewer
  - Highlighter
  - Red Curtain
  - Web Historian
  - First Response
- Resources
  - M-trends
  - forums.mandiant.com
  - M-unition
    - blog.mandiant.com
- Education
  - Black Hat classes
  - Custom classes
- Webinar series
  - Sign up

MANDIANT IOC Editor

- www.mandiant.com/products/free_software/ioce/
- Just updated!
- Schemas
- XML and XSLT examples
- Import and export data to and from IOCs
- Much, much more!





M-Trends 2011

Download the full report

http://www.mandiant.com

SwA Forum 2011: APT Panel

Ryan Kazanciyan, Principal Consultant
ryan.kazanciyan@mandiant.com