

# Stop the Maelstrom: Using Endpoint Sensor Data in a SIEM to Isolate Threats

**Jody C. Patilla**

**The Johns Hopkins University**

Session ID: TECH-107

Session Classification: Intermediate

**RSACONFERENCE2012**

# Objectives

- Get more out of tools you already have
- Target known attack-related activity
- Narrow the search space for investigations
- Get defenders out of the weeds and onto the target faster
- Automate more of the process

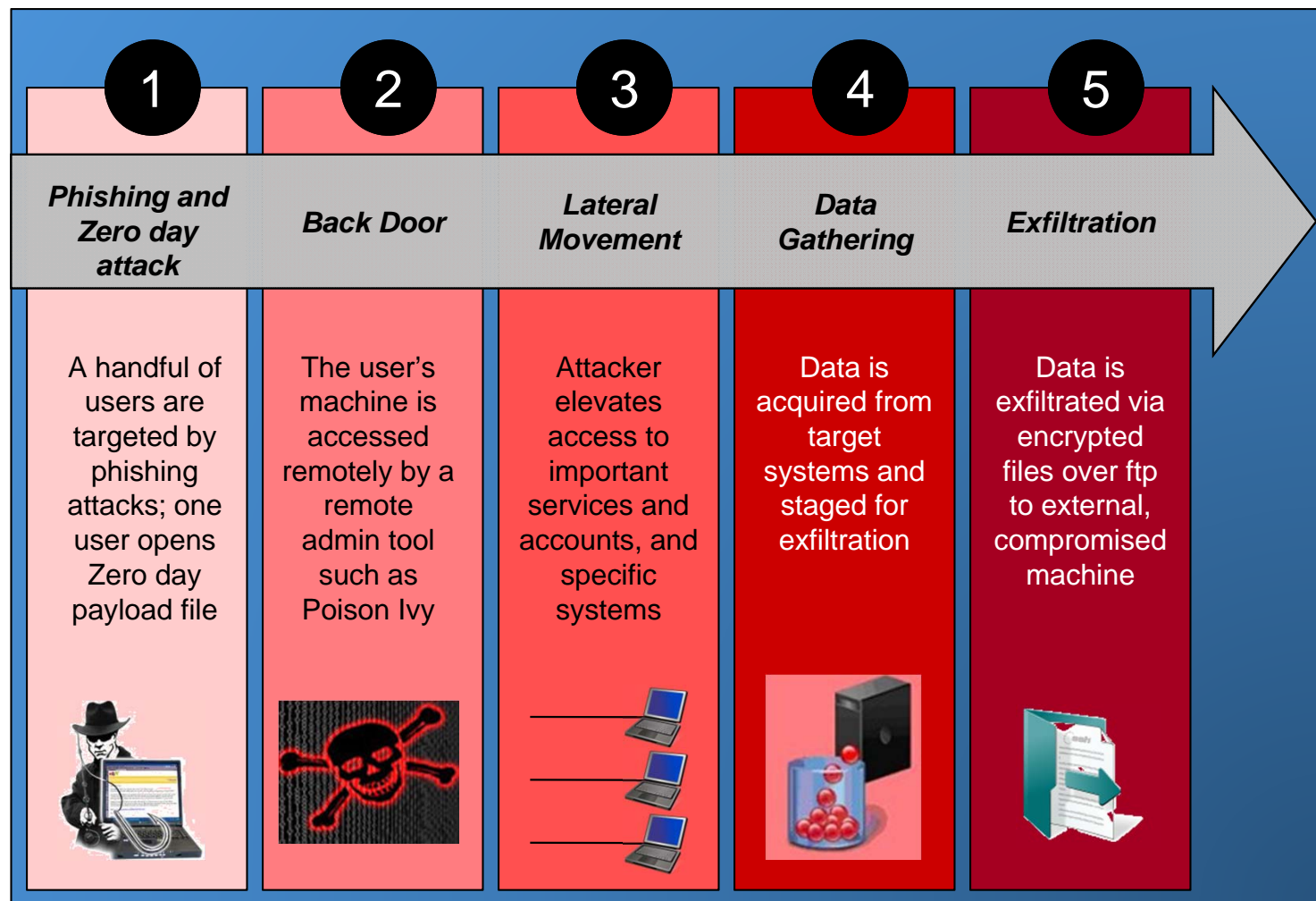


# About Johns Hopkins

- Dynamic, open culture, environment
- Under constant attack by advanced and persistent threats
- Hundreds of millions of events enter the SOC every day
- Limited security staff to manage large set of resources



# Profile of an Advanced Threat

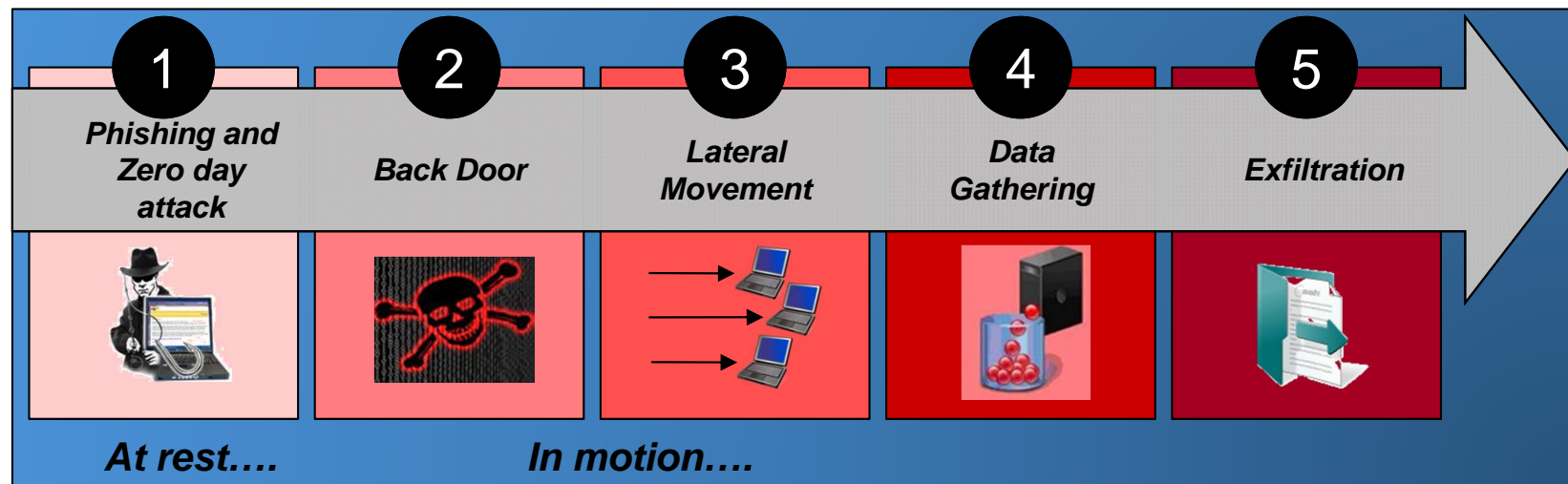


- Highly targeted
- Establishes foothold on endpoint
- Can remain dormant for months
- Controlled by a remote operator
- Targets your most valuable IP and assets
- Hide in plain sight



# Challenges for Defenders

- Too much data, too little time, not enough analysts
- Most data is captured in motion, on the wire; most attacks hit the endpoint
- Post-event forensics a nightmare of needles and haystacks
- Near-real time correlation of endpoint and network events could be a force multiplier



# Endpoint Sensor Intelligence



## Real Time File Intelligence

- Arrival of every new executable or script file
- File name, path, hash, type, reputation and other metadata
- Timestamp, Target host, IP address
- User name, process name, installer



## Removable Device Intelligence

- Vendor, device name, serial number
- Timestamp, Target host, IP address



## Configuration and Memory Monitoring

- Define traps on any registry setting or configuration file
- Monitor any cross process memory access or injection



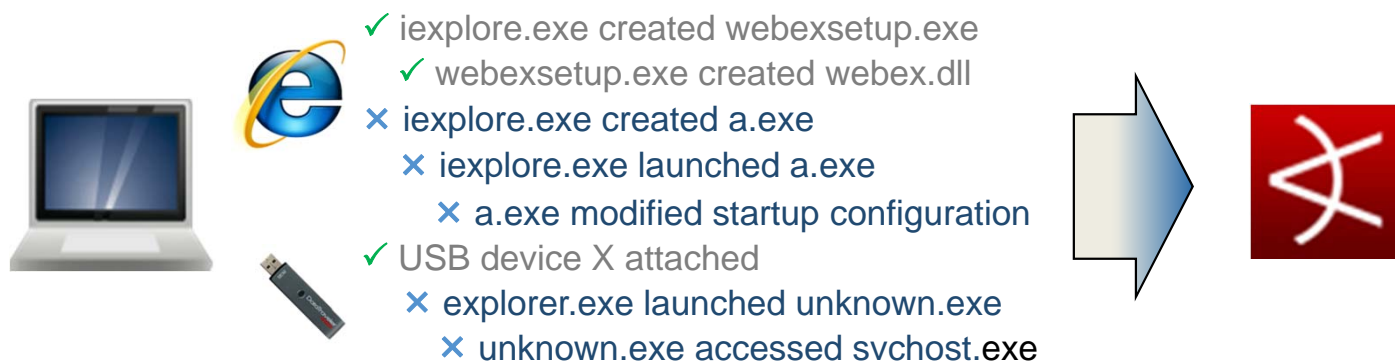
## Inventory and Propagation Intelligence

- Where else does the file exist in my organization
- What other files has it created



# Providing Better Threat Indicators

- Whitelisting technology provides deeper near real-time visibility into endpoint activity (in addition to proactive defensive capabilities)
- The endpoint sensor becomes a means to filter out noise
- Visibility into all unapproved file and process activity, and targeted configuration and memory activity
- Data is available even if malware removes its tracks
- Reputation services can augment filters with threat and trust indicators



# Endpoint InfoSec Events

Event ID	Message	Description	Significance
1201	Malicious file detected	File with high threat has been detected based on Bit9 software reputation service	Standalone
1200	Potential risk file detected	Potentially unwanted file has been detected based on Bit9 software reputation service	Standalone
1004	Banned file written to computer	Explicitly blocked file (name and/or hash) detected. [active process, installer, ...]	Standalone
802	Execution block (banned file)	Explicitly blocked file attempted execution.	Standalone
1009	Device attached	USB with file system attached. [vendor, device]	Correlate
1003	New pending file to computer	Unapproved file detected. [file, hash, installer, ...]	Correlate
1007	First execution on network	Never before seen file executed. [file, hash, installer, ...]	Correlate
800	Tamper protection blocked	Attempt to stop security service, or modify/delete files or configuration. [user, process, ...]	Correlate
305	Multiple failed logins	Three consecutive login failures	Standalone
[Future]	Registry / memory / file traps	Specific traps can be defined on any file, registry or cross process memory activity	Standalone





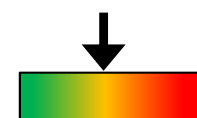
# Correlation with Other Devices

Description	ids1	fw	ips	ids2	dns	av	intel	Bit9
Time	•	•	•	•	•	•		•
Event ID	•	•	•	•	•	•		•
Name								•
Message								•
End Point Mode								•
File Name				•		•	•	•
File Hash				•		•	•	•
Process Name						•		•
Device Custom String2								•
File Path								•
Local Host		•			•	•		•
User Name								•
Local IP	•	•	•	•	•	•		•
Function								•
Remote Host/Domain				•	•		•	
Remote IP	•	•	•	•	•		•	



# Assessing Risk Against Attack Patterns

- Track entry vectors of attacks
  - USB devices
  - EXE download over the wire
- Track arrival of unapproved executables
  - New pending files
- Look for suspicious indicators
  - The parent process is an unlikely install vector
  - The file is trying to hide itself
  - The file matches known intelligence indicators
- Track new file executions
- Correlate with suspicious outbound traffic



# Detection and Correlation Use Cases

- Examples for handling standalone and correlated events
- Basic use case format:
  1. Example event is generated at endpoint and/or on network, and sent to SIEM
  2. Event passes current SIEM filters
  3. New SIEM rule triggers given selected condition
  4. Can tie to previously observed activity
  5. Action and/or notification generated



# Detection: Alternate Data Streams (ADS)

- Windows Hidden file attached to normal file
- Originally created for NTFS compatibility with Macintosh OS Resource Fork
- Some malware hides executables in ADS files
- ADS Filename resembles – good.exe:bad.exe
  - Where good.exe is known but the related good.exe:bad.exe is HIDDEN.
  - Utilities are generally needed to list ADS files in directories
  - To execute the ADS, the call must be: “start {fullpath}\goodfile.exe:bad.exe”



# Detection: New Executable is an ADS

## Endpoint Sensor

1. Sends New File Event to SIEM

## SIEM

2. Filter passes endpoint New File events
3. Rule triggers if filename contains ":" and does not start with "<fileid:"
4. Action sends Notification: "ADS File"

## Benefit

Anomalous files associated with malware automatically flagged



# Detection: New EXE File written by Atypical Process

## Endpoint Sensor

1. Sends New File Event to SIEM

## SIEM

2. Filter passes New File events
3. Rule triggers if New File is an EXE and the Creation Process is not a typical Process
4. Action sends Notification: "New EXE written by Anomalous Process"

## Benefit

Files of dubious origin are automatically flagged



# Detection/Correlation: Tracking New Endpoint External Drives

## Endpoint

1. User attaches new device to PC
2. Sensor sends Device Attached Event to SIEM

## SIEM

3. Filter passes Event
4. Rule triggers and...
5. Associated Action writes record to Active List (Active List record = PC IP address and attached Device info)

## Benefit

The SIEM Active List can be used to correlate the origin of new malware with a file introduced from a physical device



# Detection/Correlation: Tracking New Internet Downloads

## IDS

1. User downloads EXE to PC
2. IDS sends EXE Download E4 to SIEM

## SIEM

3. Filter passes event
4. Rule triggers and...
5. Associated Action writes record to Active List
6. Active List record = PC IP address, Remote Site IP address

## Benefit

SIEM can correlate the appearance of new malware with a file downloaded from the Internet





# Correlation: Actionable Events with Drop Vector

## Endpoint Sensor

1. Sends Actionable Event to SIEM

## SIEM

2. Filter passes Actionable events
3. Rule compares User/Endpoint IP address to records in lists “Device attached” and “IDS EXE Download”
4. If Rule triggers, Action sends Notification “Actionable Event with Device Attached or EXE Download”

## Benefit

SIEM can correlate, in real-time, the origin of new malware introduced into the environment by a new drive or Internet download



# Correlation: Actionable Events with Blocked Outbound Activity

## FW/DNS

1. Sends Deny event to SIEM

## SIEM

2. Filter passes Outbound Deny events
3. Rule compares Intranet Source IP with Active List records of Endpoints with New Files
4. If Rule triggers, Action sends Notification: “Outbound Traffic Blocked with New File”

## Benefit

SIEM can correlate new blocked outbound activity with new files on the endpoint – could be linking malware with exfiltration attempt



# How to Apply in Your Environment

Within three months from this presentation, you should

- Identify the events your endpoint tool can detect and report
- Select cases for maximum bang for the buck (use our examples!)

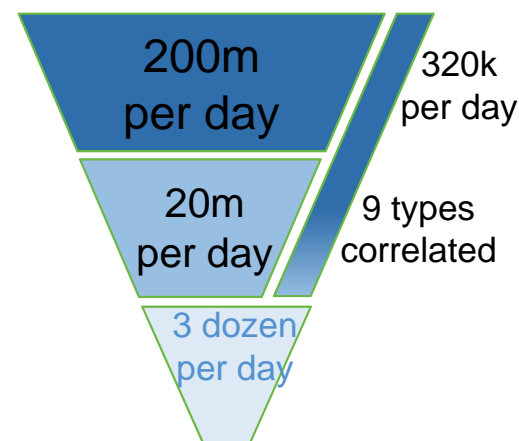
Within six months, you should

- Implement appropriate SIEM rules
- When further investigation is required, have single click access to...
  - All recent activity on target machine
  - Detailed information about suspect file (where is it, who created it, what other files did it drop, trust level of file, ...)



# Wins for You

- Extended detection of new threats and attacks
  - Detection based on new indicators
  - Detection of malware “at rest” versus “in motion”
- Reduce signal-to-noise ratio: More accurate filtering
  - Escalate severity of suspicious network activity based on actual endpoint activity
  - Correlation with ID/IPS and firewall to identify suspicious attack vectors yields a more complete picture
- Reduce time to investigate
  - Use endpoint events to gain more insight into suspicious activity
  - Console integration for investigation and analysis from single pane



Impact mean time to threat conclusion by removing endpoint blind spot



# Questions?



Jody C. Patilla

Sr. Information Assurance Analyst  
The Johns Hopkins University

jody dot patilla at jhuapl dot edu



# Examples

The following examples from our ArcSight server show how the filters, rules, and actions are implemented to address two cases discussed today: Alternate Data Streams (ADS) and a specific Internet executable download.



# ADS Example: Filter and Rule

## Filter

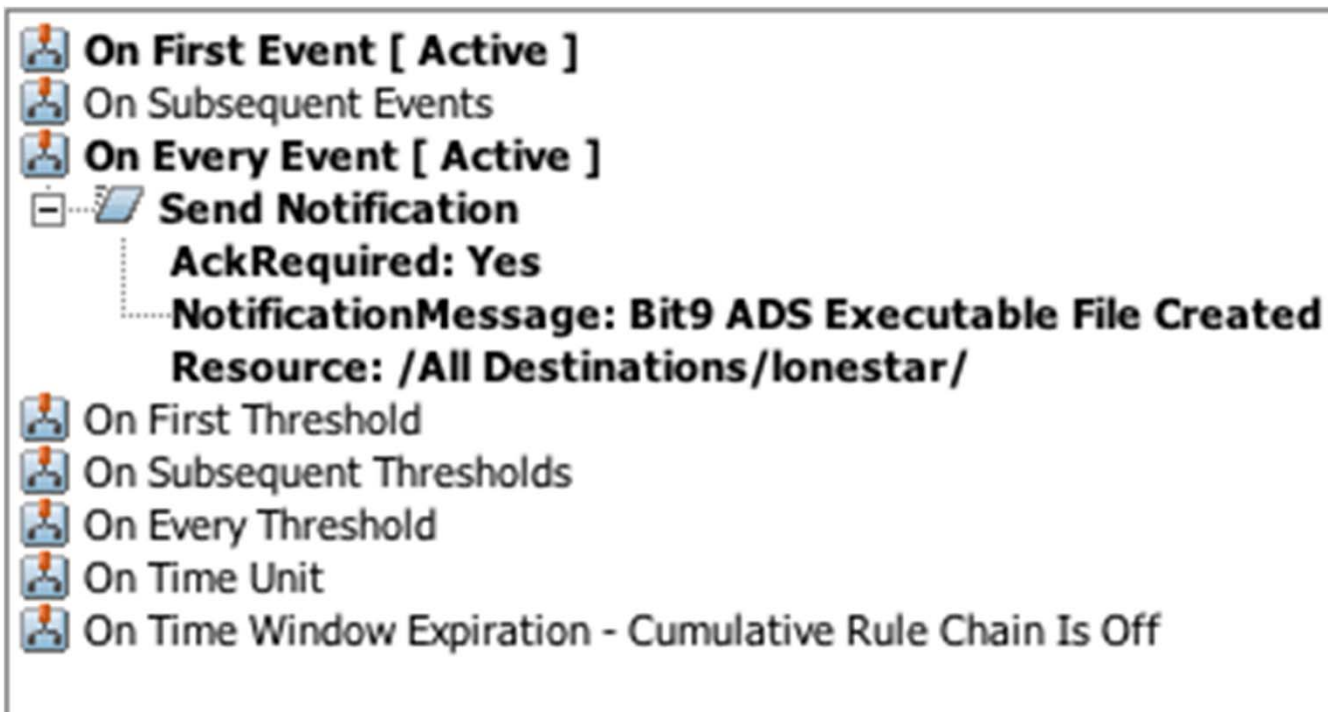


## Rule












# ADS Example: Associated Action

## Rule -> Action



The screenshot displays a list of actions for an ADS rule. The actions are:

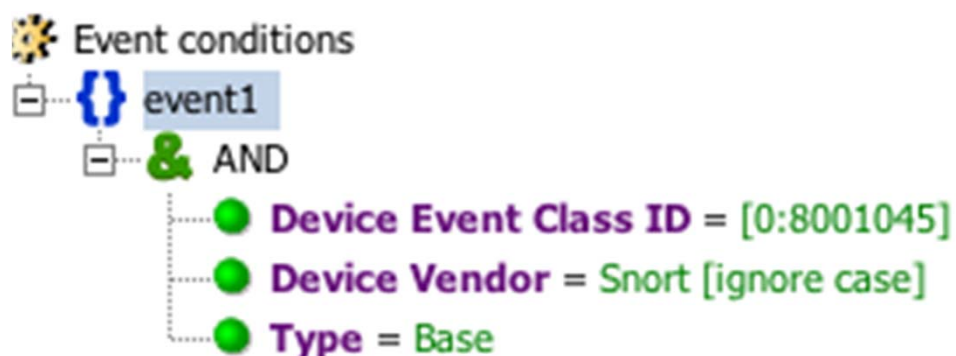
-  **On First Event [ Active ]**
-  On Subsequent Events
-  **On Every Event [ Active ]**
-  **Send Notification**
  - AckRequired: Yes**
  - NotificationMessage: Bit9 ADS Executable File Created**
  - Resource: /All Destinations/lonestar/**
-  On First Threshold
-  On Subsequent Thresholds
-  On Every Threshold
-  On Time Unit
-  On Time Window Expiration - Cumulative Rule Chain Is Off





# Snort Download Example: Filter and Rule

## Filter



## Rule



# Snort Download: Associated Action

## Rule -> Action

-  **On First Event [ Active ]**
-  On Subsequent Events
-  **On Every Event [ Active ]**
-   **Add To Active List**
  - Field: Target Address**
  - Field: Target Host Name**
  - Field: Attacker Address**
  - Field: Attacker Host Name**
  - Resource: /All Active Lists/Watch/bit9/ALL Snort PE exe download**
-  On First Threshold
-  On Subsequent Thresholds
-  On Every Threshold
-  On Time Unit
-  On Time Window Expiration - Cumulative Rule Chain Is Off

