

MISP-ECOSYSTEM

Threat Intelligence, VMRay and MISP

14-Dec-16

Koen Van Impe – koen.vanimpe@cudeso.be

Agenda

- Threat Intelligence
 - IoCs
 - TLP
 - Integrate SIEM
- MISP
 - Distribution model
 - False positives & Whitelists
 - Modules
- VMRay
- Use Case
 - E-mail with attachment



Threat

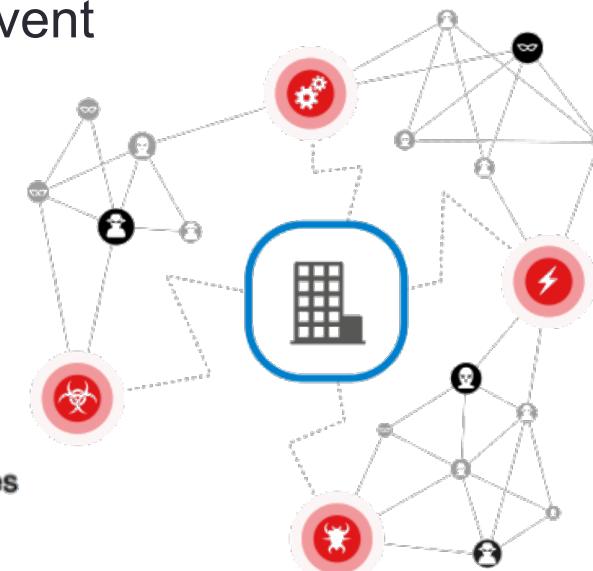
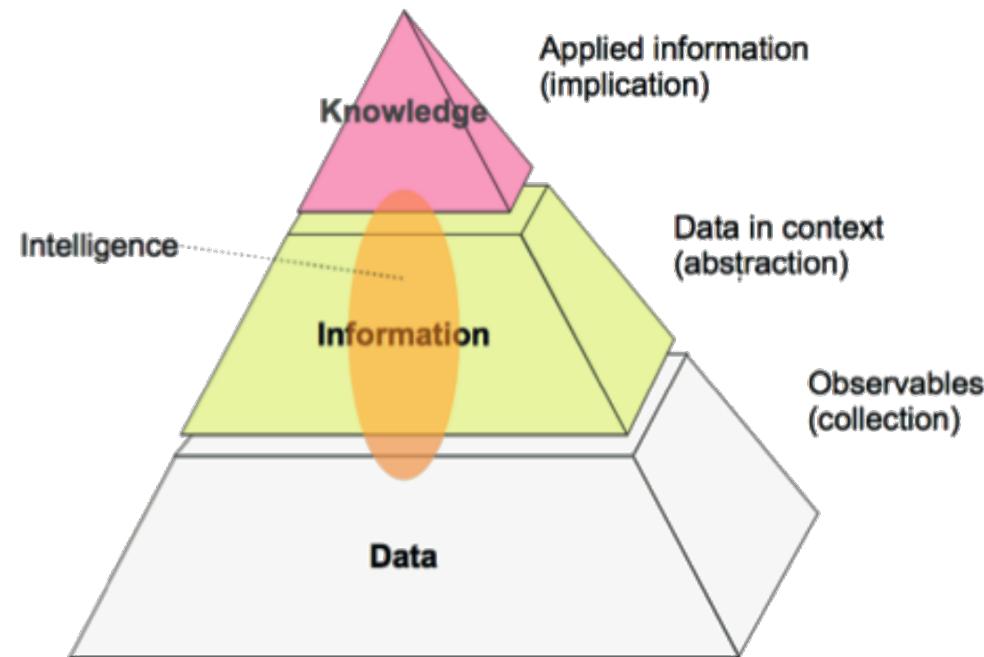
- What is a **Threat**?

- an expression of intent to do harm, i.e. deprive, weaken, damage or destroy;
- an indication of imminent harm;
- an agent that is regarded as harmful;
- a harmful agent's actions comprising of tactics, techniques and procedures (TTPs).



Intelligence

- What is **Intelligence**?
 - Information that provides **relevant** and **sufficient understanding** for **mitigating** the **impact** of a harmful event

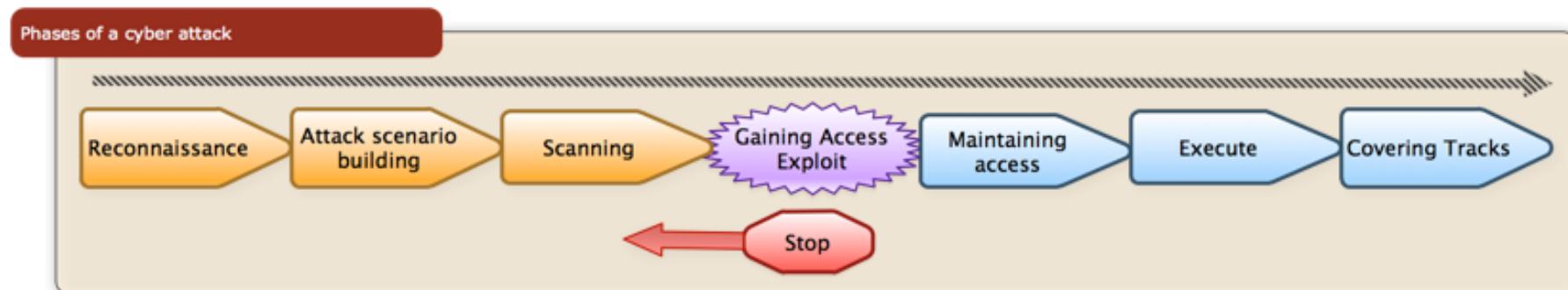


Threat Intelligence

- What is Threat Intelligence?
 - Information about threats and threat actors that provides relevant and sufficient understanding for mitigating the impact of a harmful event

Threat Intelligence

- Why do you need Threat Intelligence?
 - First step in protecting your business
 - **Understand** exposure to threats
 - Expanded attack surface
 - **Weigh defenses** towards threats
 - **Actionable** instead of noise
 - Get ahead of the game

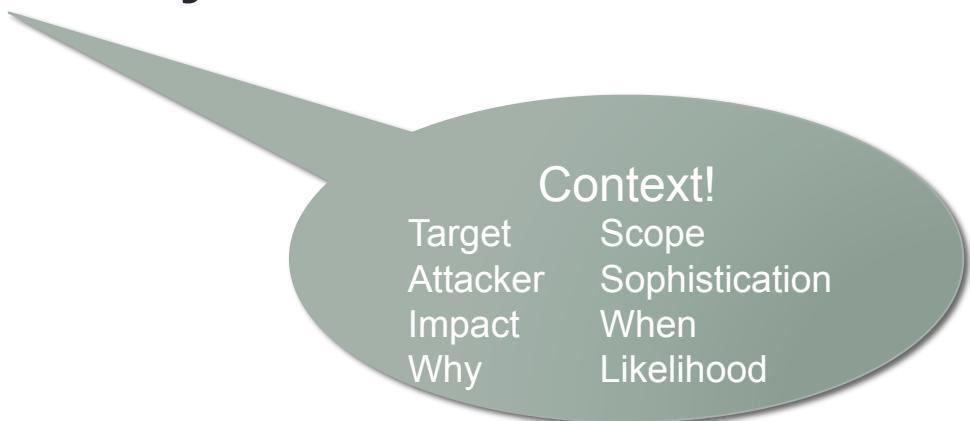


Threat Intelligence & SIEMs

- Insight on network, applications, servers and users
- SIEMS without threat feeds
 - Difficult to remove the noise, needle in a haystack
- Why consume threat data in a SIEM?
 - Faster, others do the research, you consume
 - Instead of "a" connection-> "**the**" connection
 - Fills the blind spots –correlate- things you didn't know
 - Not "auto-magic-correlation"
 - Additional context
 - Prioritize
 - Incidents
 - Vulnerability management

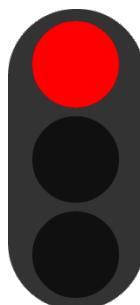
Indicator of Compromise - IoC

- Threat intelligence is more (TTPs!) than just IoCs
 - But that's how it's most often used
- Information to identify **potentially** malicious behavior
 - IPs
 - Careful with shared hosting
 - Domain names
 - URLs
 - File hashes
 - High confidence
 - Registry keys
 - Mutex



Audience : Traffic Light Protocol - TLP

- When and how (threat) information can be **shared**
- Not a classification scheme
- <https://www.first.org/tlp>

**RED**

Strong limited
Not for disclosure
Participants only
Mostly verbally or in person

**GREEN**

Relaxed, known by the inner-circle
The community
Not via publicly accessible channels

**AMBER**

Limited, people that act on the information
Restricted to participants' organizations

Sources are at liberty to specify
additional intended limits of the sharing

**WHITE**

Open, known by everyone
Disclosure is not limited
Standard copyright rules

Threat Intelligence Platforms

- Lots of buzz (fuss)
- Marketing
- Vendor driven <-> What you really need



Defense in derpth™

Maximum protection from threatening threaty threats like

One of the Koreas

Threat Intelligence Platforms

- <https://www.vanimpe.eu/pewpew/index.html?pew=1>



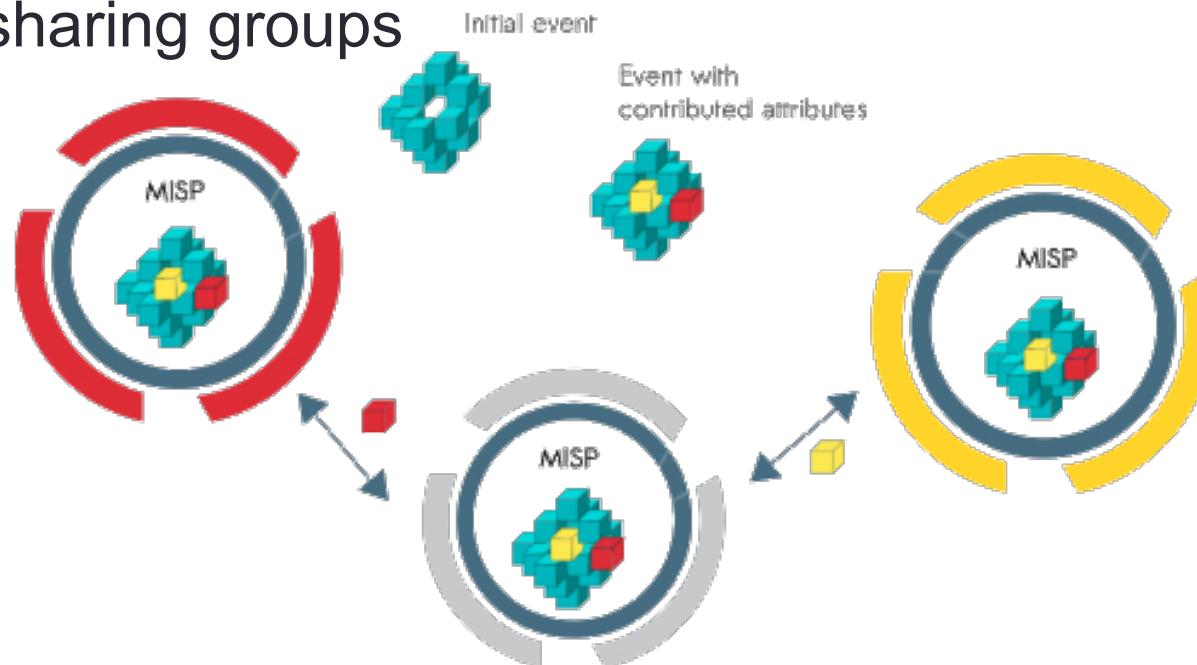
MISP - Malware Information Sharing Platform & Threat Sharing

- Started 2012
- Christophe Vandeplas
 - CERT for Belgian MoD
- <https://github.com/MISP/MISP>
- <http://www.misp-project.org/>



MISP – Information Sharing

- Distributed sharing model
 - Everyone can be a consumer or contributor
 - Based on practical user feedback
- Quick benefit : no obligation to contribute
- Different sharing groups



For whom?

- **Malware reversers** willing to share indicators of analysis with respective colleagues.
- **Security analysts** searching, validating and using indicators in operational security.
- **Intelligence analysts** gathering information about specific adversary groups.
- **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
- **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
- **Fraud analysts** willing to share financial indicators to detect financial frauds.

I can't share!

- Be a **consumer**
 - MISP groups
 - Use OSINT
- Legal restrictions
 - Sharing groups and communities
- Convince management to share
 - Share without attribution ('ownership change')



BOTVRIJ.EU
POWERED BY
MISP
Threat Sharing

OSINT Feeds

- Open Source Intelligence
- Community feeds
- Set filter (import) rules

ID	Name	Feed Format	Provider	Url	Target	Publish	Delta Merge	Override IDS	Distribution	Tag	Enabled	Actions
1	CIRCL OSINT Feed	MISP	CIRCL	https://www.circl.lu/doc/misp/feed-osint		All communities				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	The Botvrij.eu Data MISP	MISP	Botvrij.eu	http://www.botvrij.eu/data/feed-osint		All communities				<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add MISP Feed

Add a new MISP feed source.

Enabled

Name

Provider

Url

Source Format
 MISP Feed
 Freetext Parsed Feed
 Simple CSV Parsed Feed

All communities

Default Tag

Filter rules:

Set pull rules

Allowed Tags

Blocked Tags

Allowed Organisations

Blocked Organisations

MISP Events & Attributes

- Events
 - "a threat", for example a new ransomware-run
 - Own events
 - From **connected** sites
 - Distribution level
 - Tagging (TLP, category, ...)
- Attributes
 - What is the threat about?
 - Sightings
 - Network, File hashes, Financial info (CC, Bitcoin)
 - Context
 - Text
 - **Correlation** with other events
 - Seen in other events?
 - **Proposals**

MISP Events & Attributes

Events

	Published	Org	Owner Org	ID	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	CUDESO	78	tip:white	20	koen.vanimpe@cudeso.be		2016-11-14	Medium	Completed	New Carbanak / Anunak Attack Methodology	All	 
✓	CUDESO	CUDESO	77	tip:white	11	koen.vanimpe@cudeso.be		2016-11-14	Low	Completed	Ransom Desktop Locking Ransomware Ransacks Local Files and Social Media Profiles	All	 
✓	CUDESO	CUDESO	76	tip:white	19	koen.vanimpe@cudeso.be		2016-11-09	Medium	Completed	Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Patched	All	 

- Multiple attributes per event

  					Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes					
	Date	Org	Category	Type	Value	Comment	Related	IDS	Distribution	Actions
<input type="checkbox"/>	2016-11-16		External analysis	link	https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Carbanak-/-Anunak-Attack-Methodology/?page=1&year=0&month=0		No	Inherit	 	
<input type="checkbox"/>	2016-11-16		Network activity	ip-dst	179.43.133.34		Imported via the Freetext Import Tool	Yes	Inherit	 
<input type="checkbox"/>	2016-11-16		Network activity	ip-dst	192.99.14.211		Imported via the Freetext Import Tool	Yes	Inherit	 
<input type="checkbox"/>	2016-11-16		Network activity	ip-dst	5.45.179.173		Imported via the Freetext Import Tool	Yes	Inherit	 

False positives



download.microsoft.com



Real False Positive

- Misconfigured sandbox
 - OS Update traffic
 - Browsers fetch CRL
 - Routing issues

Not False Positive

- Malware checks network connectivity
- Malware changes resolution of important domains

You need context

Learn TTP

Add "If Then"-logic ; infection check

- 1st : Machine visits "evil.com"
 - 2nd : Traffic to "download.microsoft.com"
 - Only traffic to "evil.com"
- } Incident Response
- } Not sure **compromised** or **resisted**; dive deeper to evaluate situation

False positives - MISP

- Recurring challenge in information sharing
- MISP introduced **warninglists**
 - lists of well-known indicators that can be associated to potential false positives, errors or mistakes
 - Enable per list
 - <https://github.com/MISP/misp-warninglists>
 - Alexa Top 100
 - Microsoft, Google domains
 - RFC 1918
- **Alert** when adding an attribute that is on the warninglist
 - You decide what to do!
 - You have to "know" the logic, MISP can not do that for you

False positives - MISP

Warninglists

« previous next »

ID	Name	Version	Description	Type	Valid attributes	Entries	Enabled	Actions
13	TLDs as known by IANA	2	Event contains one or more TLDs as attribute with an IDS flag set	string	hostname, domain, domain ip	1290	<input checked="" type="checkbox"/>	
12	Second level TLDs as known by Mozilla Foundation	2	Event contains one or more second level TLDs as attribute with an IDS flag set	string	hostname, domain, domain ip	6462	<input type="checkbox"/>	
11	List of RFC 5735 CIDR blocks	2	Event contains one or more entries part of the RFC 5735 CIDR blocks - Special Use IPv4 Addresses	cidr	ip-src, ip-dst, domain ip	15	<input type="checkbox"/>	
10	List of RFC 3849 CIDR blocks	2	Event contains one or more entries part of the IPv6 documentation prefix (RFC 3849)	cidr	ip-src, ip-dst, domain ip	1	<input type="checkbox"/>	
9	List of RFC 1918 CIDR blocks	2	Event contains one or more entries part of the RFC 1918 CIDR blocks	cidr	ip-src, ip-dst, domain ip	3	<input checked="" type="checkbox"/>	

Only show potentially false positive attributes

Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields

Key	Type	Value	Comment	Related Events	IDS	Distribution	Action
activity	hostname	download.microsoft.com	⚠ download.microsoft.com: List of known microsoft domains		Yes	Inherit	*

Whitelists - MISP

- Whitelist attributes from being added to signatures
- Company assets

The screenshot shows the 'Import Whitelist' page of the MISP web interface. At the top, there is a navigation bar with links: Home, Event Actions, Input Filters, Global Actions, Sync Actions, and Administration. Below the navigation bar, there are two main sections: 'List Whitelist' (highlighted in blue) and 'New Whitelist'. The 'Import Whitelist' section contains a table with one row. The table has columns for 'Id' and 'Name'. The first row shows an 'Id' of 1 and a 'Name' of '/belgium.be/'. Navigation buttons for 'previous' and 'next' are located above the table.

Id	Name ↓
1	/belgium.be/

Taxonomies - MISP

- Classification
 - JSON
 - ENISA, NATO, VERIS
 - Your classification
- Machine tags
 - Machines can parse it
 - Still human-readable
- Tags as filter for distribution

e-mail AG Wire payment confirmation

Event ID	2
Uuid	583b4165-77ec-4698-8c9f-79b5c0a8da15
Org	ORGNAME
Owner org	ORGNAME
Contributors	
Email	admin@admin.test
Tags	tlp:white x enisa:nefarious-activity-abuse="receiving-unsolicited-e-mail" x enisa:nefarious-activity-abuse="viruses" x veris:action:malware:vector="Email attachment" x +

Set push rules

Allowed Tags	Available Tags	Blocked Tags
tlp:red tlp:amber tlp:green	tlp:ex:chr osint:source-type="blog-p osint:source-type="techni osint:source-type="news- osint:source-type="pastie	tlp:white

Use MISP

- Web UI
 - Freetext import : large block of text ; MISP recognizes IoCs
- API access
- PyMISP
 - API'ish
- **MISP modules**
 - Import, export, extension
- MISP Galaxy
 - large object attached to a MISP event
- Taxonomies
- Workbench
 - export attributes
 - help on cases outside MISP

MISP modules

- Expansion service
 - Enrichment, Import, Export
 - Extend attributes with information from other service providers
 - Can also be your own internal provider
- Extending MISP with expansion modules with zero customization in MISP
- MISP modules can be run on the same system or on a remote server
- <https://github.com/MISP/misp-modules>

MISP modules

- ASN history
- Passive DNS
- Passive SSL
- CVE
- DNS
- PassiveTotal
- Shodan
- Virustotal
- STIX
- VMRay

VMRay

- **Agentless**
- Hypervisor based malware analysis
- OEM Integration
 - Embedded into security appliances

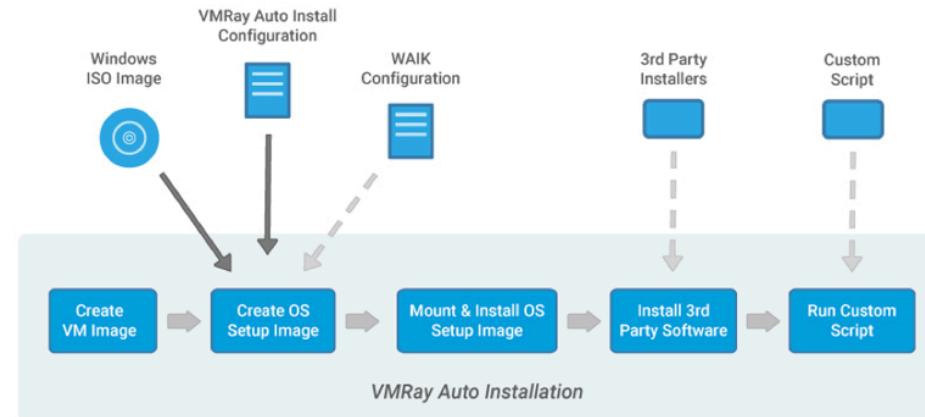
- Windows
 - 32b/64b
 - 64b kernel rootkits (Turla)
 - exe, pdf, docx, swf

The screenshot displays the VMRay interface with several key components:

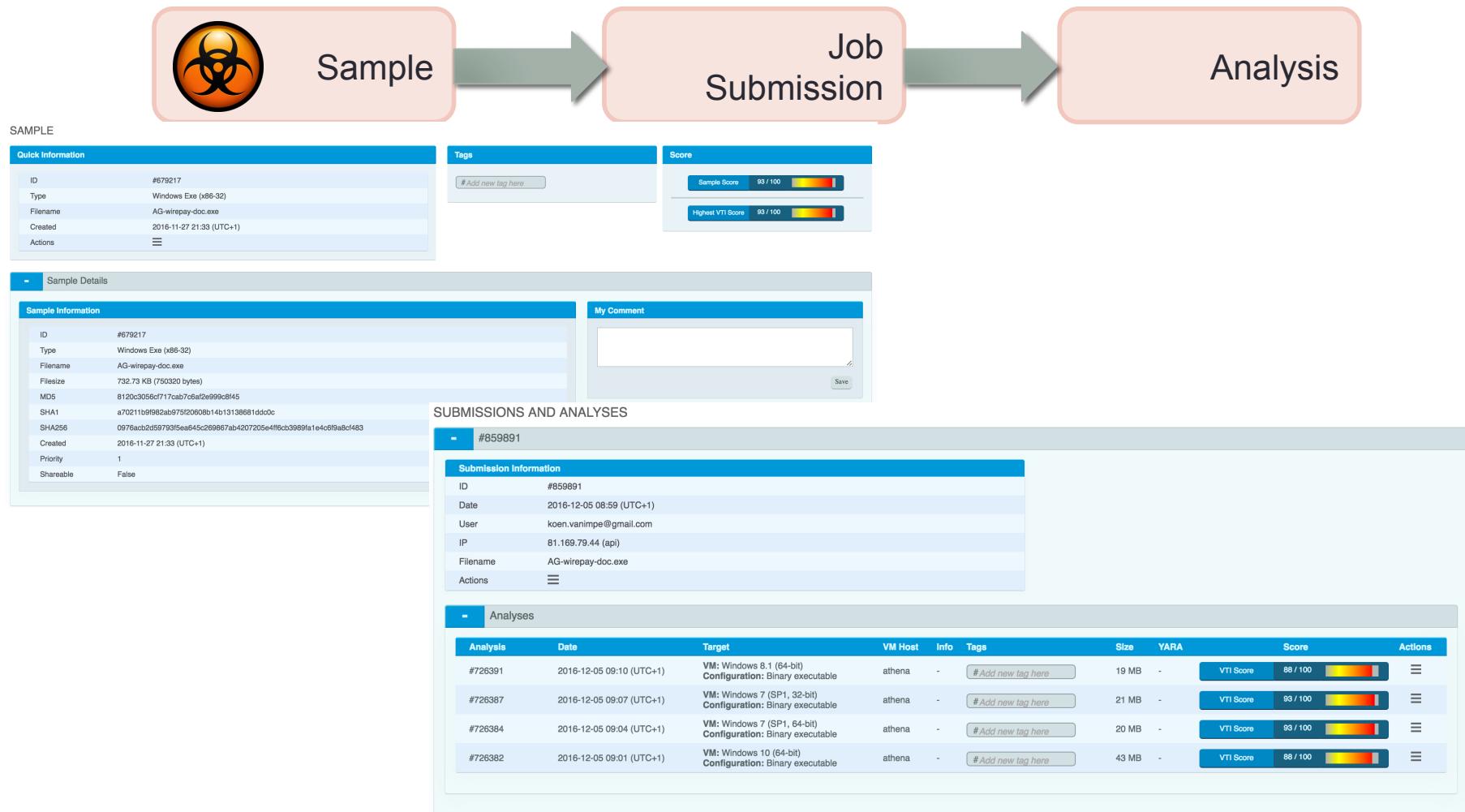
- Process Graph:** A complex directed graph showing the relationships between various processes and system components during analysis.
- VTI SCORES:** A bar chart showing the VTI Scores for different samples over time. The Y-axis ranges from 0 to 30, and the X-axis shows dates from 2016-11-28 to 2016-12-05. The legend indicates: Low (light gray), Medium (red), and High (dark red). The chart shows a high score (Medium) on 2016-11-28, a low score (Low) on 2016-11-30, and a high score (High) on 2016-12-04.
- MY ACCOUNT:** User information and job statistics. It includes fields for User (koen.vanimpe@gmail.com), Account (cudeyo.be), Samplesets (cudeyo.be), and three buttons for Queued Jobs (0), Running Jobs (0), and Analyses (-).
- SUBMISSIONS AND ANALYSES:** A table showing submission details and analysis status. It includes columns for Sample, Analysis Status, and Score. One entry is highlighted with a yellow background: "2016-12-05 08:59 AG-wirepay-doc.exe #679217 win8.1_64.exe Finished win7_32_sp1.exe Finished win7_64_sp1.exe Finished win10_64.exe Finished". A progress bar at the bottom right indicates a "Highest VTI Score" of 93 / 100.

VMRay

- Analysis in different VMs
 - Windows
 - Popular office software
 - Custom
- Extract IoCs
 - Hashes, Mutex
 - Network information
- STIX
- JSON-output
- API
 - Submit, Retrieve results
 - Automation



VMRay - Process



MISP EcoSystem



Malware



Network



Threat Info



Forensic data



TTP



Finance / Fraud



IoC



Enrichment



API



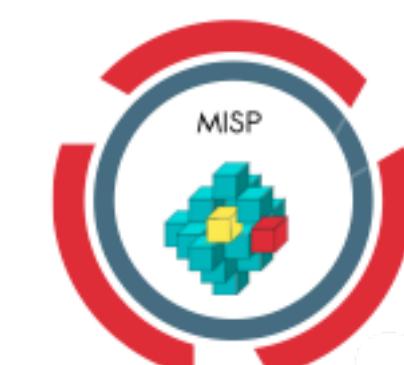
Import/Export



IR Platforms



Security devices



Use Case : E-mail with malware

From Nicharee Preedatana <davis@chinaunion-shipping.com>

Subject AG Wire payment confirmation

To info@cudeso.be

24/11/16 00:04

Hi,

Please find attached the wire payment confirmation paying invoices:

160969
LT10069
LT10072
LT10071
LT10070

Thank you

.

Nicharee Preedatana
Controller

Attachment: AG Wire payment confirmation.doc.z

AG Wire payment confirmation.doc.z:

RAR archive data, v1d, os: Win32

MD5 (AG Wire payment confirmation.doc.z) =
56c8abc137aea9e497bee0ebe61d7286

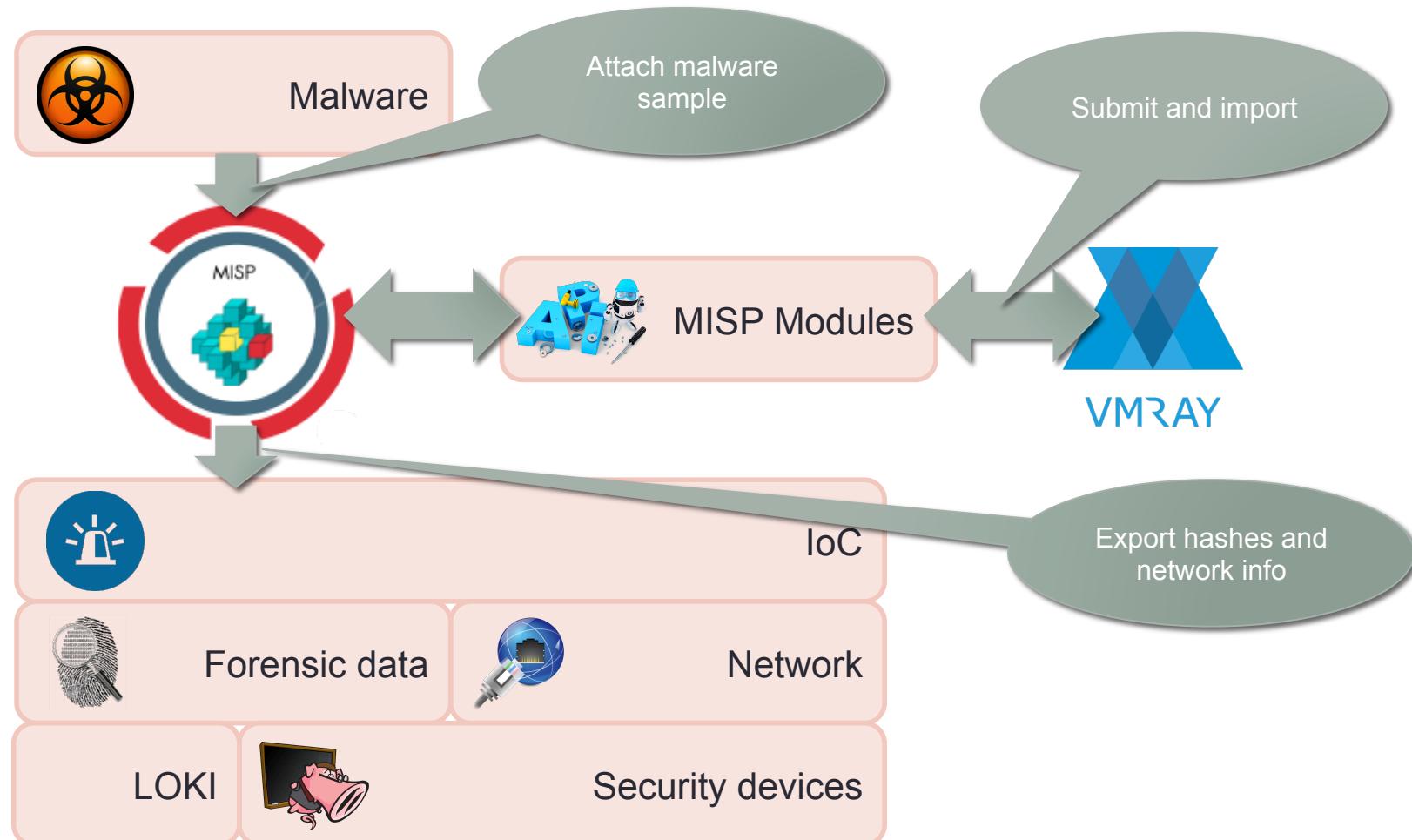
Extract : AG-wirepay-doc.exe

	AG-wirepay-doc.exe	
0	4D5A9000 03000000 04000000 FFFF0000 B8000000 00000000 40000000	
28	00000000 00000000 00000000 00000000 00000000 00000000 00000000	
56	00000000 B0000000 0E1FBA0E 00B409CD 21B8014C CD215468 69732070	
84	726F6772 616D2063 616E6E6F 74206265 2072756E 20696E20 444F5320	
112	6D6F6465 2E0D0D0A 24000000 00000000 C9E107DB 8D806988 8D806988	
140	8D806988 BBA66488 8C806988 52696368 8D806988 00000000 00000000	
168	00000000 00000000 50450000 4C010300 88703658 00000000 00000000	

Use Case : E-mail with malware

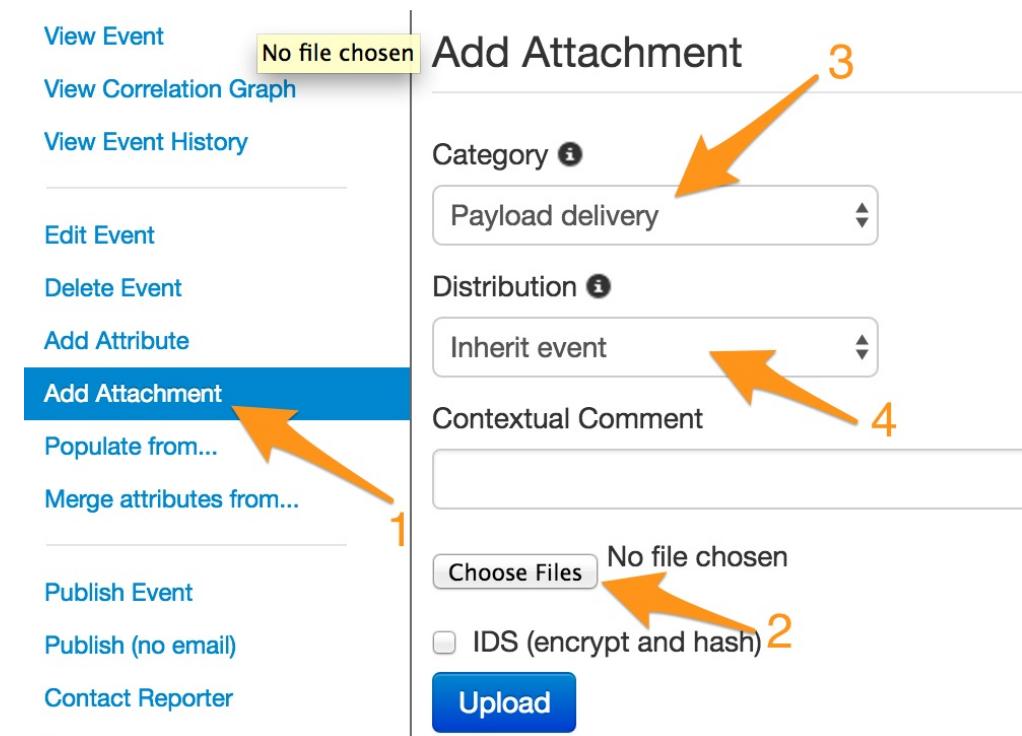
- We can use **static** analysis
 - limited
 - obfuscated
 - resource intensive
- Use malware sandboxes
 - automated analysis
 - behavior
 - careful with malware that does sandbox evasion / detection

Use Case : MISP and Malware



Step 1: Attach malware sample

- Two types of attachment in MISP
 - "Regular" attachments
 - **Payload Delivery**
 - **Antivirus Detection**
 - IDS flag not set
 - Direct downloadable from UI
 - Malware samples
 - **Artifacts Dropped**
 - **Payload Installation**
 - **IDS** flag set
 - Download via password protected ZIP



Step 1: Attach malware sample

AddAttachment_orig.mov

Step 2: Submit sample to VMRay

- Via MISP-modules Enrichment

The screenshot shows the MISP interface with several panels:

- Left Panel (View Event):** Contains links like View Correlation Graph, View Event History, Edit Event, Delete Event, Add Attribute, Add Attachment (with an orange arrow labeled 2 pointing to it), Populate from..., Merge attributes from..., and Publish Event.
- Main Panel (Events List):** A table showing event details. One row is highlighted with an orange arrow labeled 1 pointing to the "Value" column. The table includes columns for Date, Org, Category, Type, Value, and various inheritance and enrichment status indicators.
- Bottom Panel (Enrichment Results):** A table listing enriched attributes. It includes columns for Value, Similar Attributes, Category, Type, IDS, Comment, and Actions. An orange arrow labeled 1 points to the "Similar Attributes" column for the first row. Another orange arrow labeled 2 points to the "Submit" button at the bottom left.
- Bottom Buttons:** Update all comment fields and Change all.

Step 2: Submit sample to VMRay

Submit_orig.mov

Step 3: Wait for analysis

- VMRay does its magic
- Current MISP-VMRay connector is **asynchronous**
 - Submit
 - Wait for analysis to complete
 - Import
 - (work in progress)

Step 4: Import results

- Via MISP-modules **Import**
 - Based on VMRay sample ID
 - Do not forget to set IDS flag
 - (pending issue request)

Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic detection.

Value	Similar Attributes	Category	Type
Allocate a page with PAGE_EXECUTE_READWRITE permission.		Other	text
Change the protection of a page from writable (PAGE_READV)		Other	text
knofxara	1	Artifacts dropped	mutex
Create mutex with name knofxara.		Other	text
One thread sleeps more than 5 minutes.		Other	text
Change the protection of a page from writable (PAGE_READV)		Other	text
Resolve more than 50 APIs.		Other	text
wfygcseuzhmvt		Artifacts dropped	mutex
Create mutex with name wfygcseuzhmvt.		Other	text
Enable privilege SeDebugPrivilege.		Other	text
Change the protection of a page in a foreign process from wr		Other	text
Change the protection of a page from writable (PAGE_READV)		Other	text
Create more than 50 files.		Other	text

Vmray Import

Sample_id

The VMRay sample_id

666709

Include textdesc

Include textual description

Only network info

Only include network (src-ip, hostname, domain, ...) information

Include analysisid

Include VMRay analysis id text

Import

Step 4: Import results

Import_orig.mov

Consume results in SIEM

- API / PyMISP (Python access via API)
- Import feed
 - Select tags
 - Type, priority, impact
 - Set categories
 - Based on tags
- Post sightings back to MISP

Consume results in NIDS

- Malware analysis revealed network IoCs
 - Low confidence when it concerns shared hosting IPs

- Generate NIDS rules 
- automatic or manual

Snort 0 seconds ago Click this to download all network related attributes that you have access to under the Snort rule format. No N/A Completed. [Download](#) [Generate](#)

Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.

- Set of SNORT rules

```
alert udp any any -> any 53 (msg: "MISP e2 Domain: dadabada.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|08|dadabada|03|com|00|"; fast_pattern; nocase; classtype:trojan-activity; sid:4036541; rev:1; priority:3; reference:url,http://MISP/events/view/2;)
alert tcp any any -> any 53 (msg: "MISP e2 Domain: dadabada.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|08|dadabada|03|com|00|"; fast_pattern; nocase; flow:established; classtype:trojan-activity; sid:4036542; rev:1; priority:3; reference:url,http://MISP/events/view/2;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e2 Outgoing HTTP Domain: dadabada.com"; flow:to_server,established; content: "Host|3a|"; nocase; http_header; content:"dadabada.com"; nocase; http_header; pcre: "/(^[^A-Za-z0-9-])dadabada\.com[^A-Za-z0-9-\.]/H"; tag:session,600,seconds; classtype:trojan-activity; sid:4036543; rev:1; priority:3; reference:url,http://MISP/events/view/2;)
```

End-point investigation

- YARA rules
 - Signature based detection
- File hashes
 - High confidence
 - Slow
 - Get files
 - Investigate
 - High reward
 - Use perimeter sandbox
 - Before delivery
 - Queued

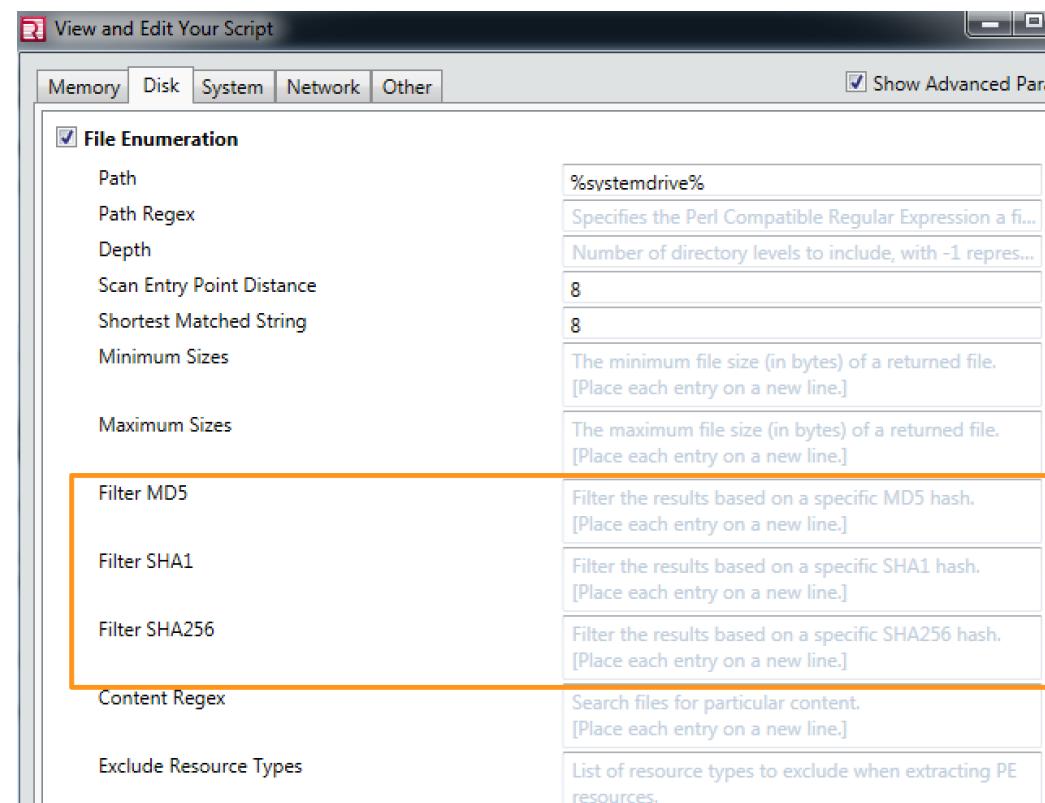
End-point investigation

- Loki
 - <https://github.com/Neo23x0/Loki>
 - Fetch YARA rules from MISP
 - File hashes

```
[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Scanning C:\ ...
-[ALERT] Malware Hash TYPE: SHA256 HASH: b12c7d57507286bbbe36d7acf9b34c22
c96606ffd904e3c23008399a4a50c047 FILE: C:\$Recycle.Bin\S-1-5-21-949666807
-3097873-177000209-1000\$RC7V2PZ.sys DESC: Regin Malware Sample
[ALERT] Yara Rule MATCH: Regin_APT_KernelDriver_Generic_B FILE: C:\$Recyc
le.Bin\S-1-5-21-949666807-3097873-177000209-1000\$RC7V2PZ.sys
```

End-point investigation

- FireEye – Redline
 - Memory acquisition
 - Drive acquisition
 - Per image
 - Dedicated
 - You know the hosts in scope



End-point investigation

- Nessus
 - Plugin 65548
 - Search custom file hashes

Service: cifs

445 / tcp

```
ED870A44064799B7DCEA3F9B674D0077 matches a known malware md5sum.

File Path : c:\windows\system32\winscard.dll
Associated PID(s) during check : 364,828,4348
Description : C:\WINDOWS\system32\winscard.dll

OCBD1906F74BEB539FCEF6493095B933 matches a known malware md5sum.

File Path : c:\windows\system32\tquery.dll
Associated PID(s) during check : 3300
Description : C:\WINDOWS\system32\tquery.dll

F70E342E180436100F3797F046CCF660 matches a known malware md5sum.

File Path : c:\windows\system32\shfolder.dll
Associated PID(s) during check : 584,828,1168,3200,4732
Description : c:\WINDOWS\system32\shfolder.dll

12BCFB57162AD17CEA545E362CD886A8 matches a known malware md5sum.

File Path : c:\windows\system32\netman.dll
Associated PID(s) during check : 480,760,828,3200
Description : c:\WINDOWS\system32\netman.dll
```

MISP – The Future

- MISP Modules
 - via MISP Hackaton
- MISP Objects
 - Semi dynamic data model
 - Share the object design along with the events shared
- MISP Galaxy
 - Large object -> cluster
 - Threat actors, campaigns
- MISP Workbench
 - Use attributes outside MISP for further investigation