MISP-ECOSYSTEM

Threat Intelligence, VMRay and MISP

14-Dec-16

Koen Van Impe – koen.vanimpe@cudeso.be

Agenda

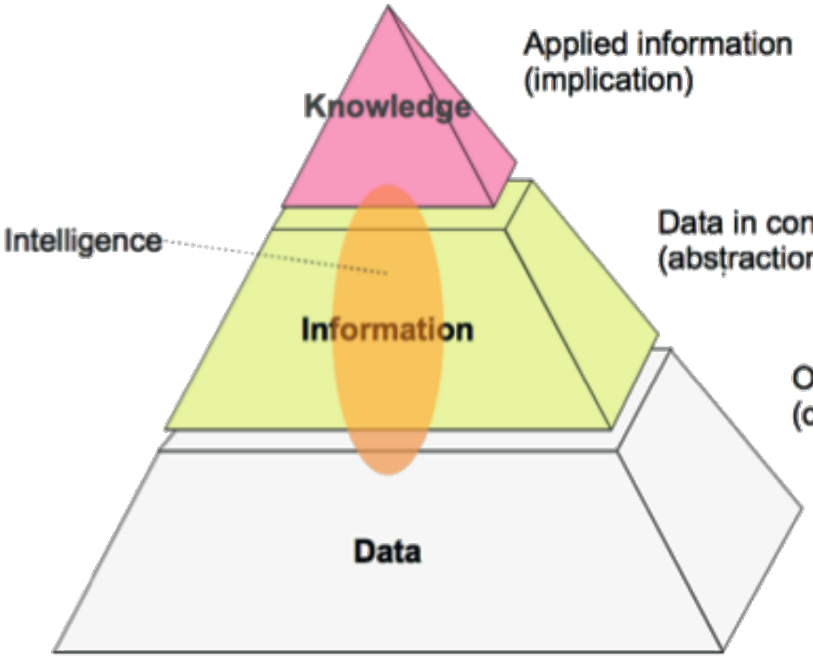
- Threat Intelligence
  - IoCs
  - TLP
  - Integrate SIEM
- MISP
  - Distribution model
  - False positives & Whitelists
  - Modules
- VMRay
- Use Case
  - E-mail with attachment

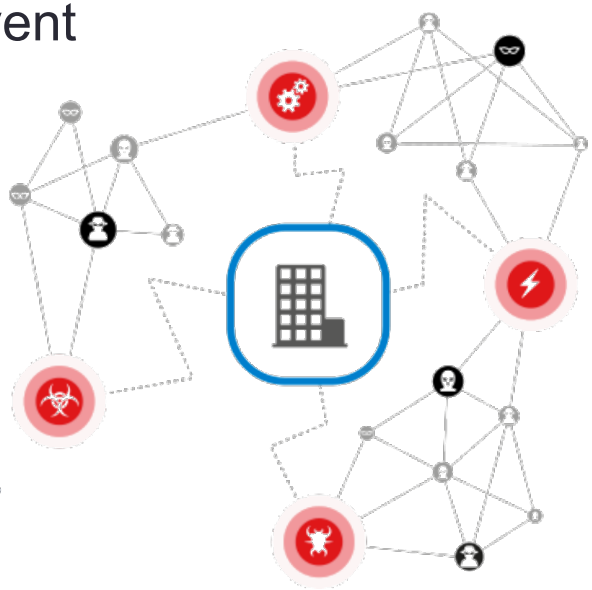
Threat

- 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



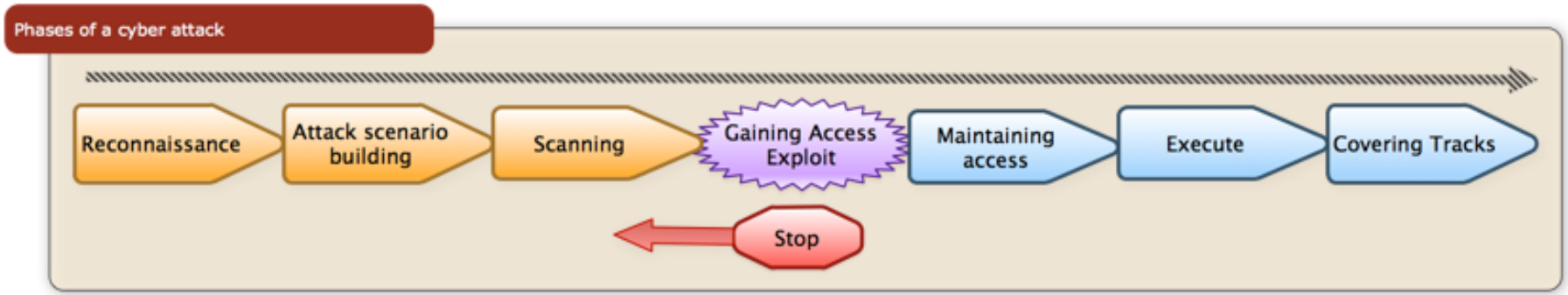


Threat Intelligence

- 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



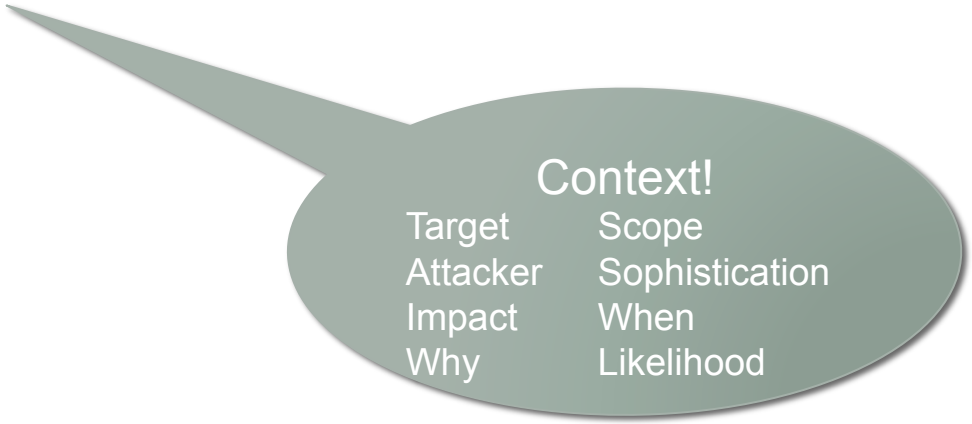
Threat Intelligence & SIEMs

- 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

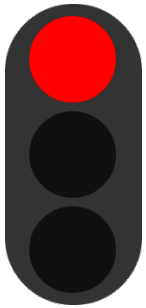
- Threat intelligence is more (TTPs!) than just IoCs
  - But that's how it's most often used

- Information to identify **potentially** malicious behavior
  - IPs
    - Careful with shared hosting
  - Domain names
  - URLs
  - File hashes
    - High confidence
  - Registry keys
  - Mutex



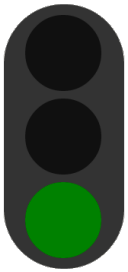
Audience : Traffic Light Protocol - TLP

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



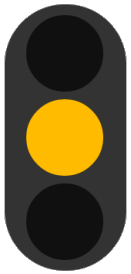
RED

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



GREEN

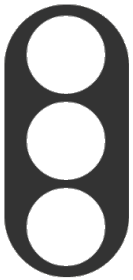
Relaxed, known by the inner-circle
The community
Not via publicly accessible channels



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

Threatbutt

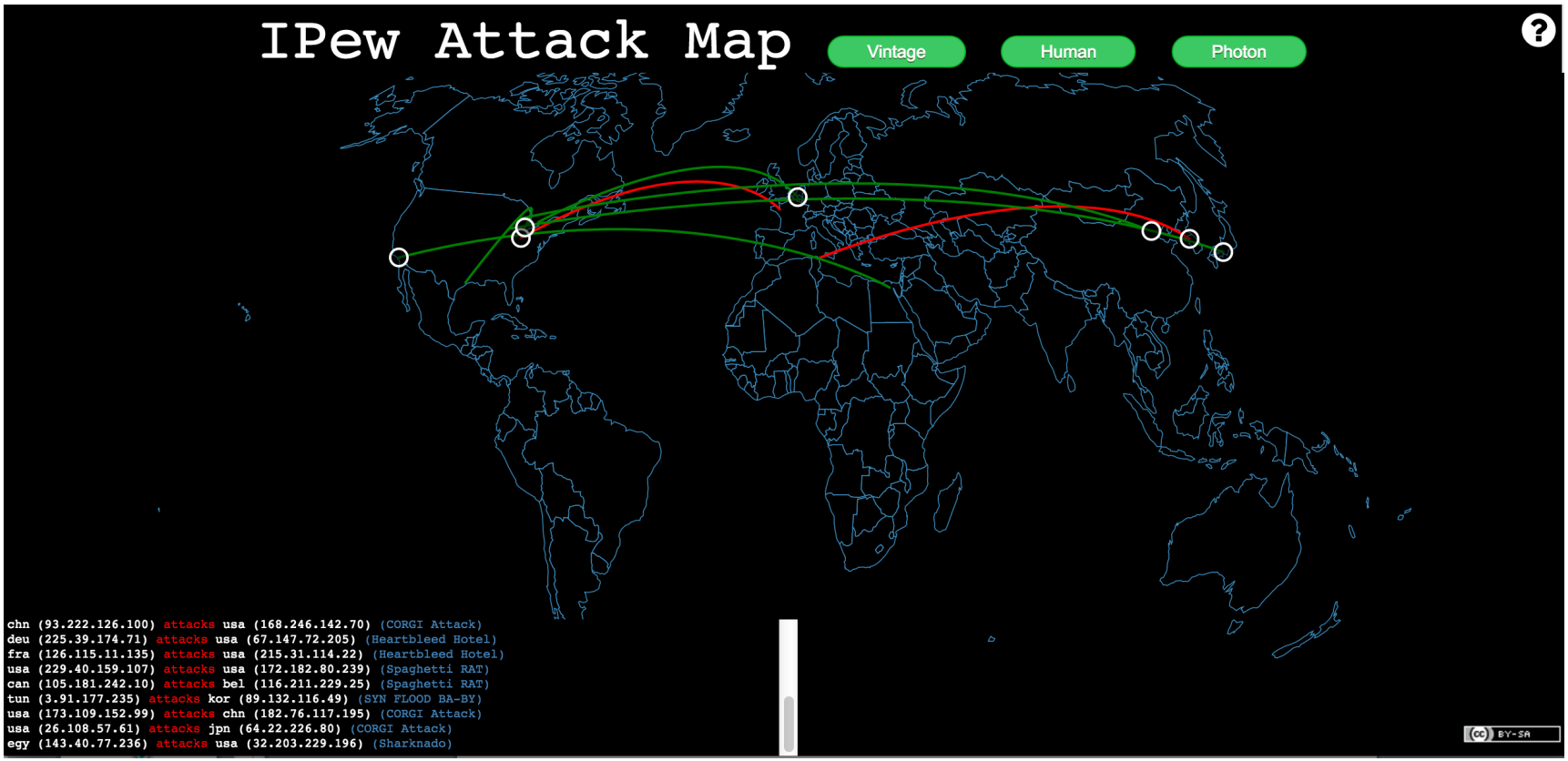
Defense in derpth™

Maximum protection from threatening threaty threats like

One of the Koreas

Threat Intelligence Platforms

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

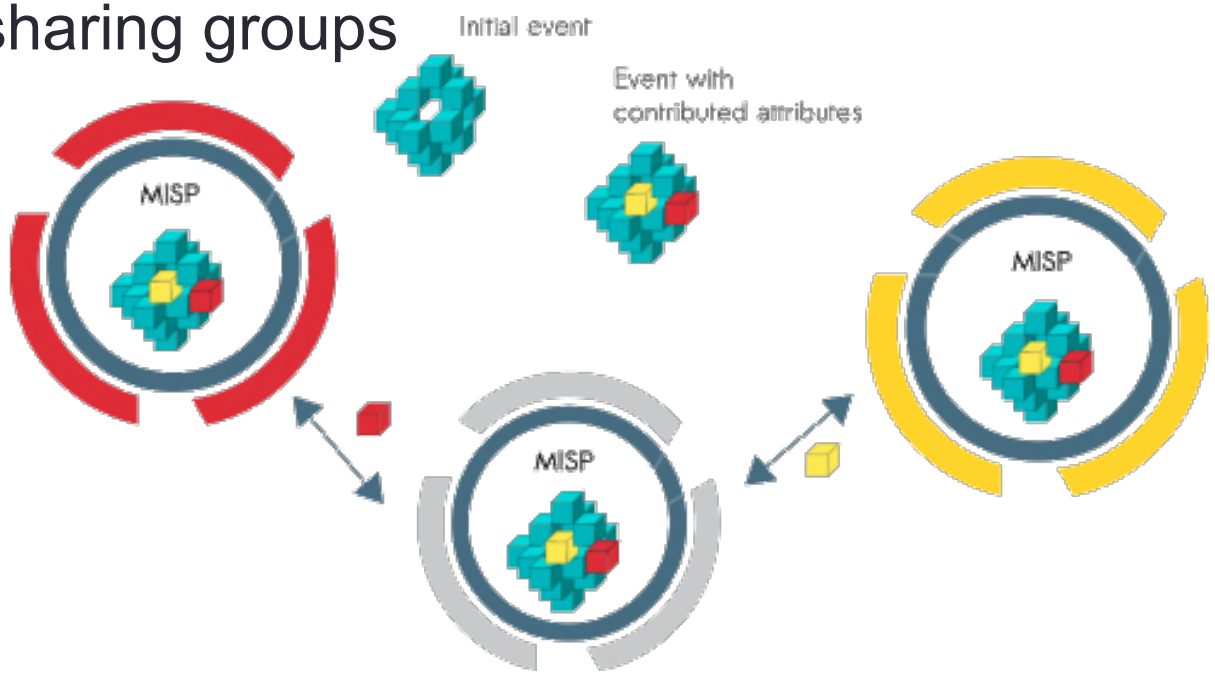


MISP - Malware Information Sharing Platform & Threat Sharing

- 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?

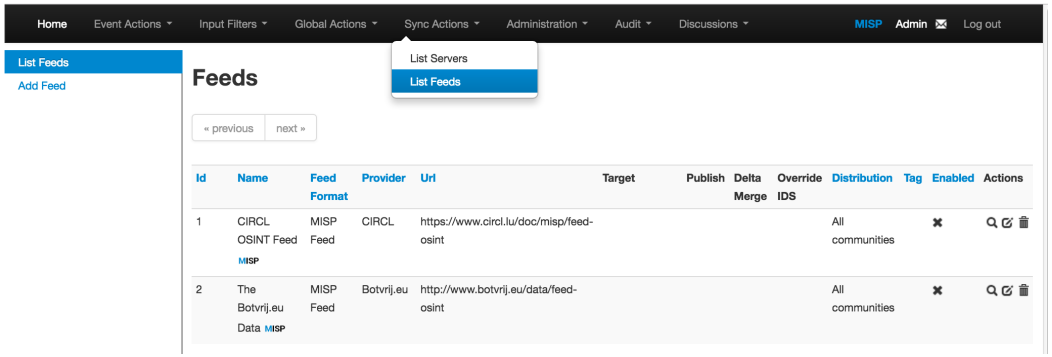
- **Malware reversers** willing to share indicators of analysis with respective colleagues.
- **Security analysts** searching, validating and using indicators in operational security.
- **Intelligence analysts** gathering information about specific adversary groups.
- **Law-enforcement** relying on indicators 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.

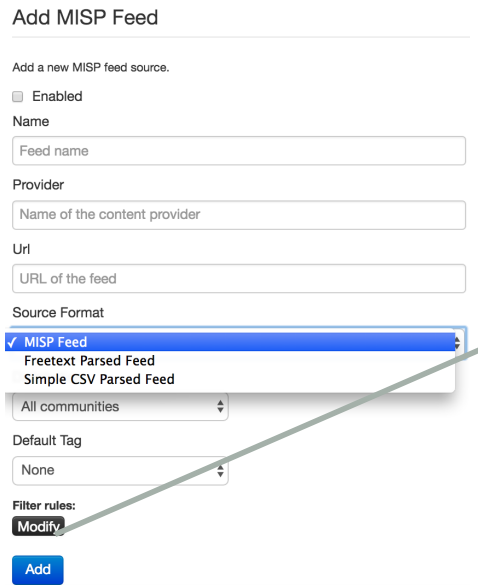
I can't share!

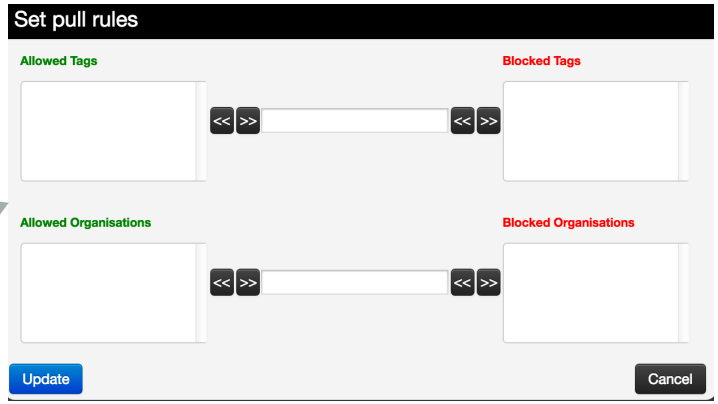
- Be a **consumer**
  - MISP groups
  - Use OSINT
- Legal restrictions
  - Sharing groups and communities
- Convince management to share
  - Share without attribution ('ownership change')

OSINT Feeds

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



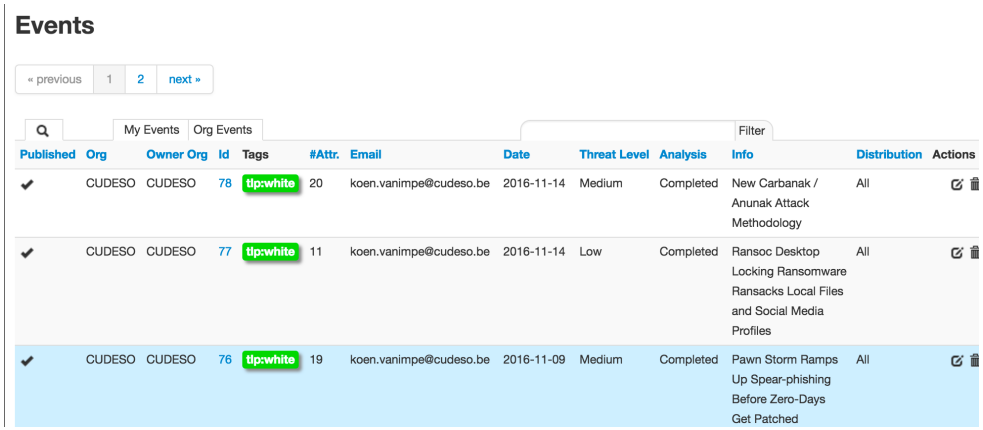




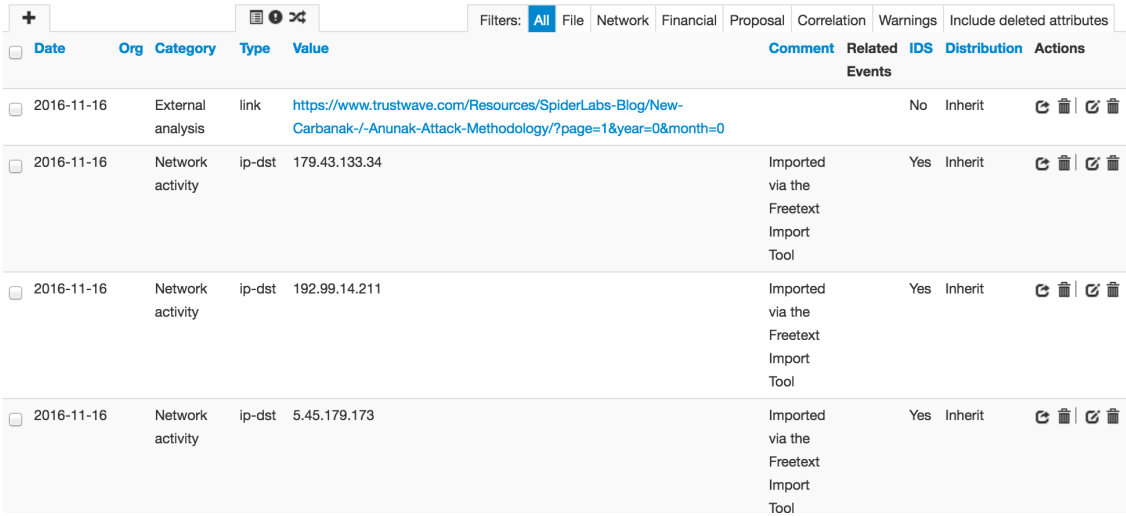
MISP Events & Attributes

- 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



- Multiple attributes per event



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"

} **Incident Response**

- Only traffic to "evil.com"

} Not sure **compromised** or **resisted;** dive deeper to evaluate situation

https://soltra.com/en/articles/the-truth-about-false-positives-and-their-root-causes-in-cyber-threat-intelligence/

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

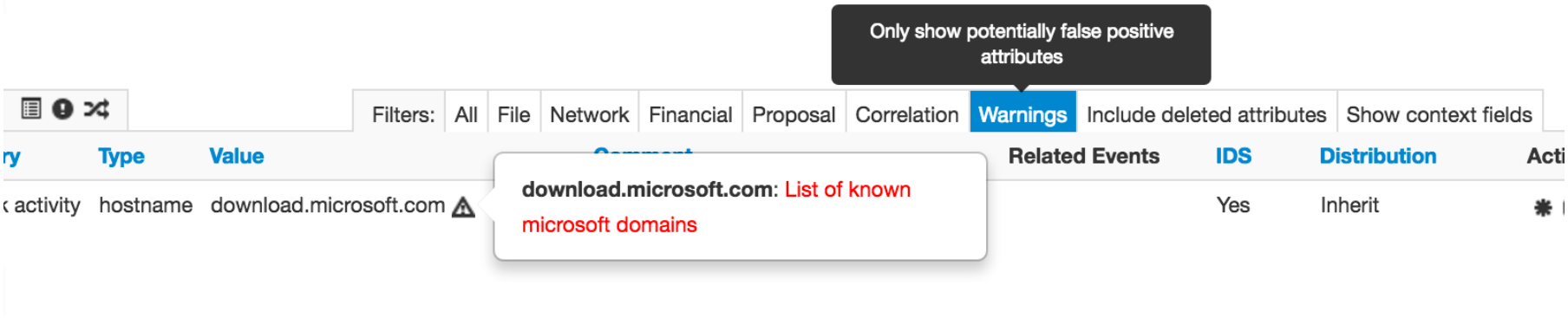
  - **Alert** when adding an attribute that is on the warninglist
    - You decide what to do!
    - You have to "known" the logic, MISP can not do that for you

False positives - MISP

Warninglists

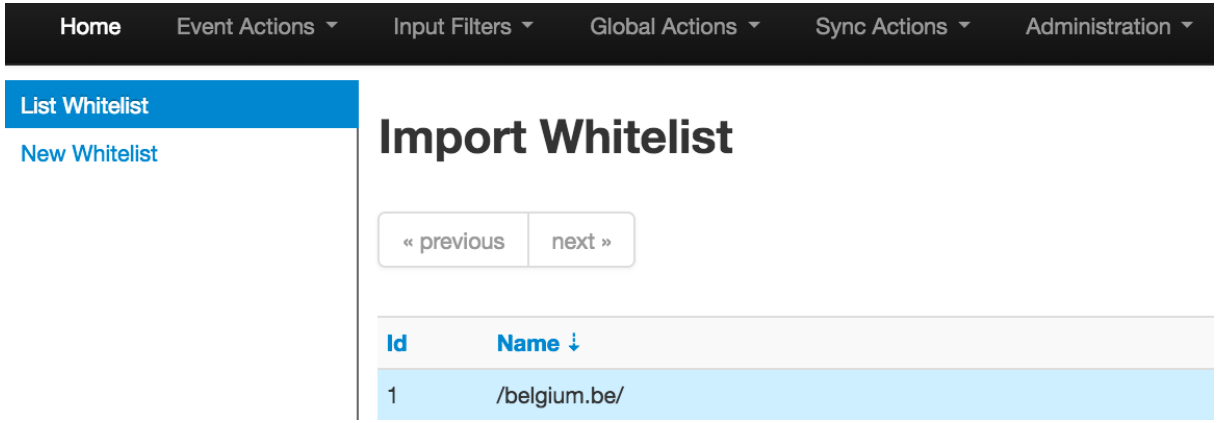
« previous | next »

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	☑	
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	☐	
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	☐	
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	☐	
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	☑	



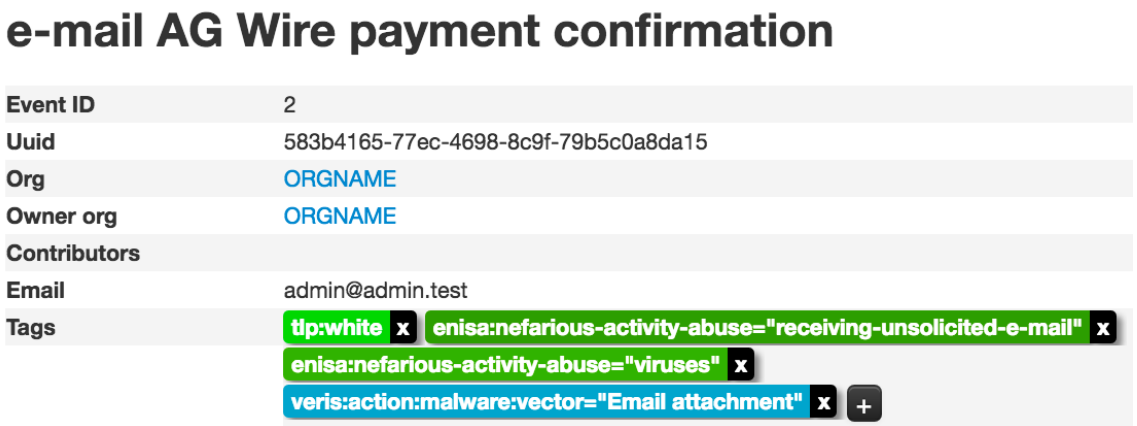
Whitelists - MISP

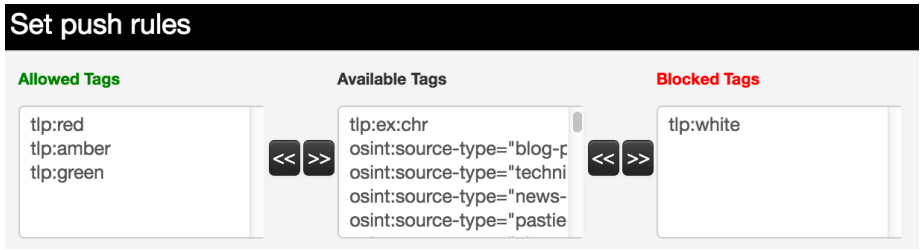
- Whitelist attributes from being added to signatures
- Company assets



Taxonomies - MISP

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





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

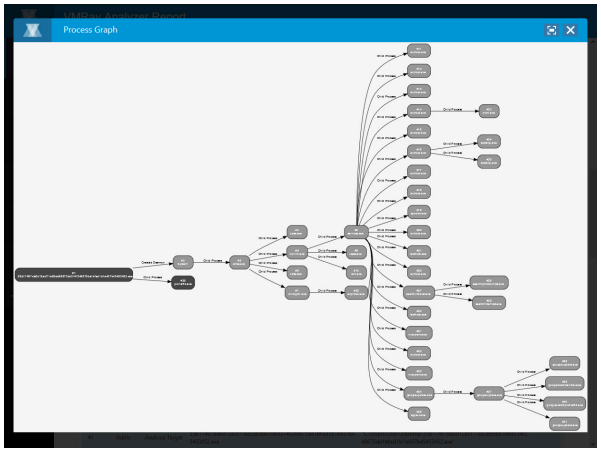
- Expansion service
  - Enrichment, Import, Export
  - Extend attributes with information from other service providers
  - Can also be your own internal provider
- Extending MISP with expansion modules with zero customization in MISP
- MISP modules can be run on the same system or on a remote server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

MISP modules

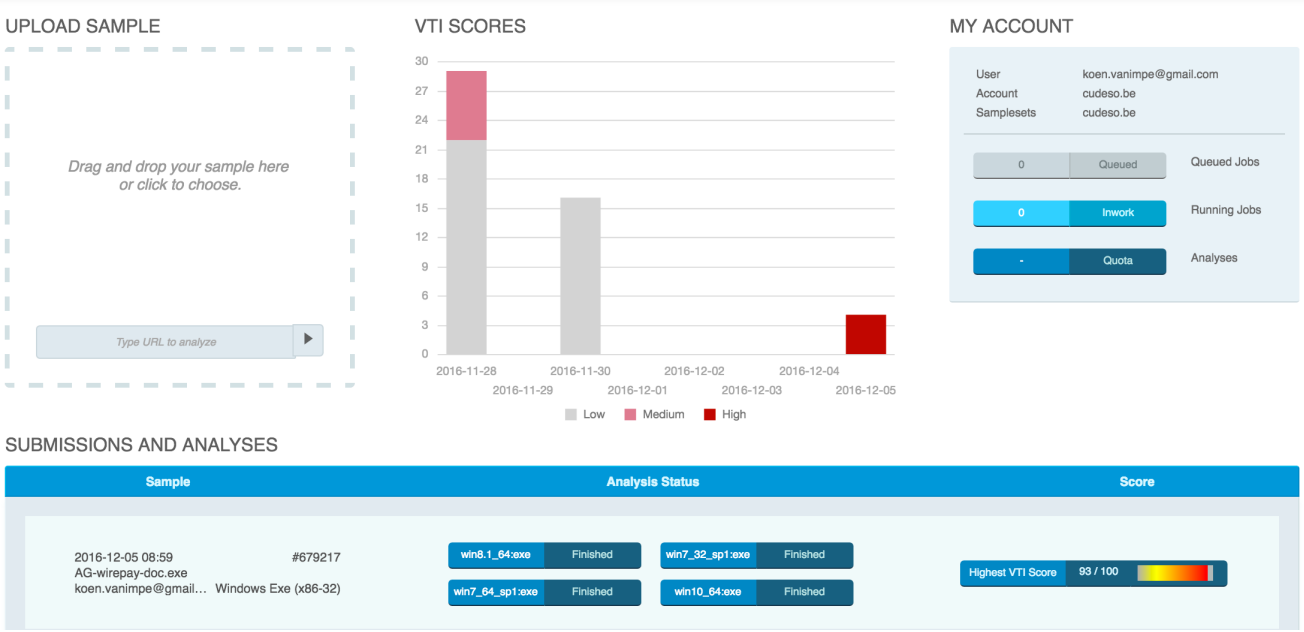
- ASN history
- Passive DNS
- Passive SSL
- CVE
- DNS
- PassiveTotal
- Shodan
- Virustotal
- STIX
- VMRay

VMRay

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

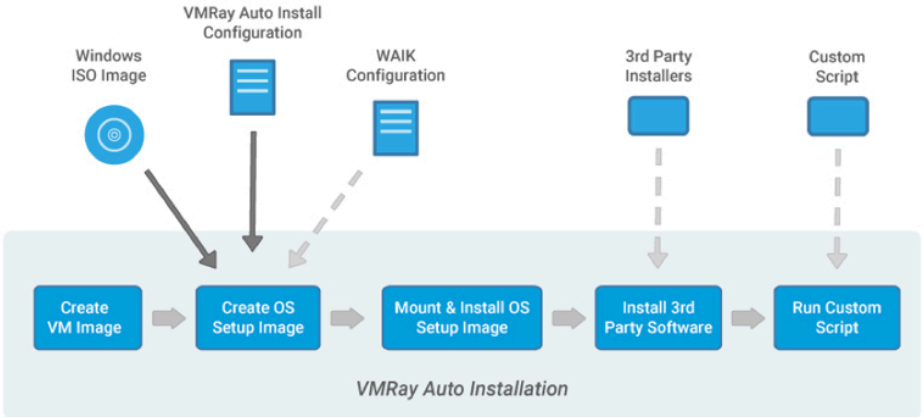


- Windows
  - 32b/64b
  - 64b kernel rootkits (Turla)
  - exe, pdf, docx, swf

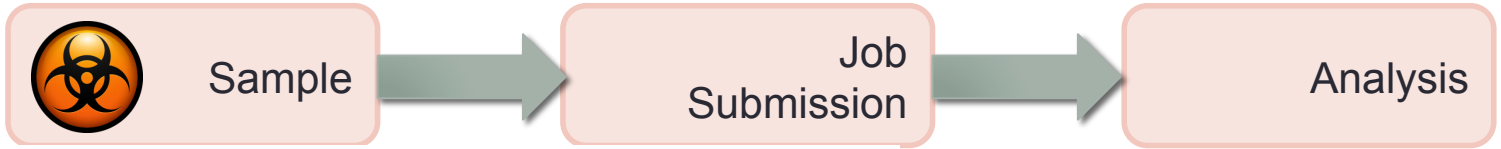


VMRay

- 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



SAMPLE

Quick Information

ID	#679217
Type	Windows Exe (x86-32)
Filename	AG-wirepay-doc.exe
Created	2016-11-27 21:33 (UTC+1)
Actions	

Tags

Add new tag here

Score

Sample Score 93 / 100

Highest VTI Score 93 / 100

Sample Details

Sample Information

ID	#679217
Type	Windows Exe (x86-32)
Filename	AG-wirepay-doc.exe
Filesize	732.73 KB (750320 bytes)
MD5	8120c3056cf717cab7c6af2e999c8f45
SHA1	a70211b9f982ab975f20608b14b13138681ddc0c
SHA256	0976acb2d59793f5ea645c269867ab4207205e4ff6cb3989fa1e4c6f9a8cf483
Created	2016-11-27 21:33 (UTC+1)
Priority	1
Shareable	False

My Comment

Save

SUBMISSIONS AND ANALYSES

#859891

Submission Information

ID	#859891
Date	2016-12-05 08:59 (UTC+1)
User	koen.vanimpe@gmail.com
IP	81.169.79.44 (api)
Filename	AG-wirepay-doc.exe
Actions	

Analyses

Analysis	Date	Target	VM Host	Info	Tags	Size	YARA	Score	Actions
#726391	2016-12-05 09:10 (UTC+1)	**VM:** Windows 8.1 (64-bit) **Configuration:** Binary executable	athena	-	# Add new tag here	19 MB	-	VTI Score 88 / 100	
#726387	2016-12-05 09:07 (UTC+1)	**VM:** Windows 7 (SP1, 32-bit) **Configuration:** Binary executable	athena	-	# Add new tag here	21 MB	-	VTI Score 93 / 100	
#726384	2016-12-05 09:04 (UTC+1)	**VM:** Windows 7 (SP1, 64-bit) **Configuration:** Binary executable	athena	-	# Add new tag here	20 MB	-	VTI Score 93 / 100	
#726382	2016-12-05 09:01 (UTC+1)	**VM:** Windows 10 (64-bit) **Configuration:** Binary executable	athena	-	# Add new tag here	43 MB	-	VTI Score 88 / 100	

MISP EcoSystem


Malware


Network


Threat Info


Forensic data

TTP


Finance / Fraud


IoC


Enrichment

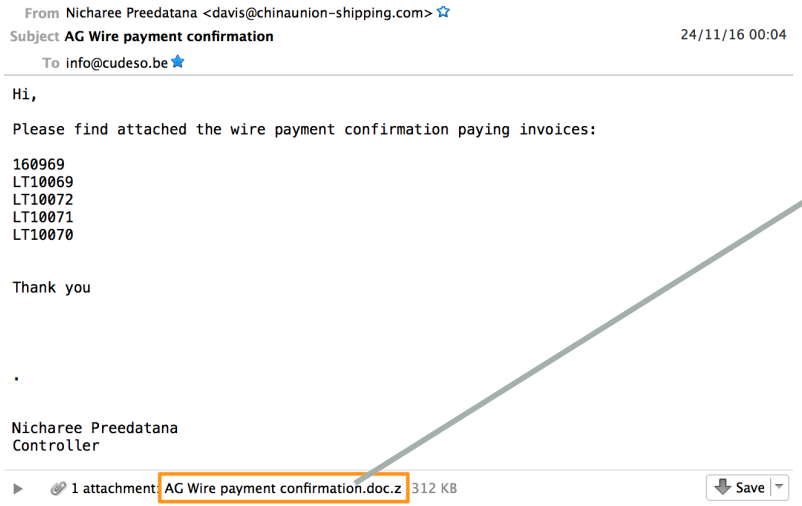

API


Import/Export


IR Platforms


Security devices

Use Case : E-mail with malware

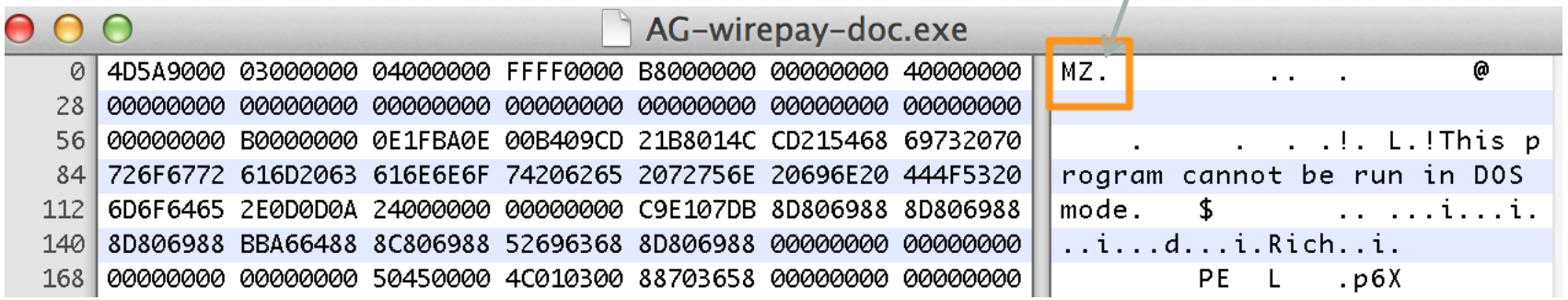


Attachment: AG Wire payment confirmation.doc.z

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**

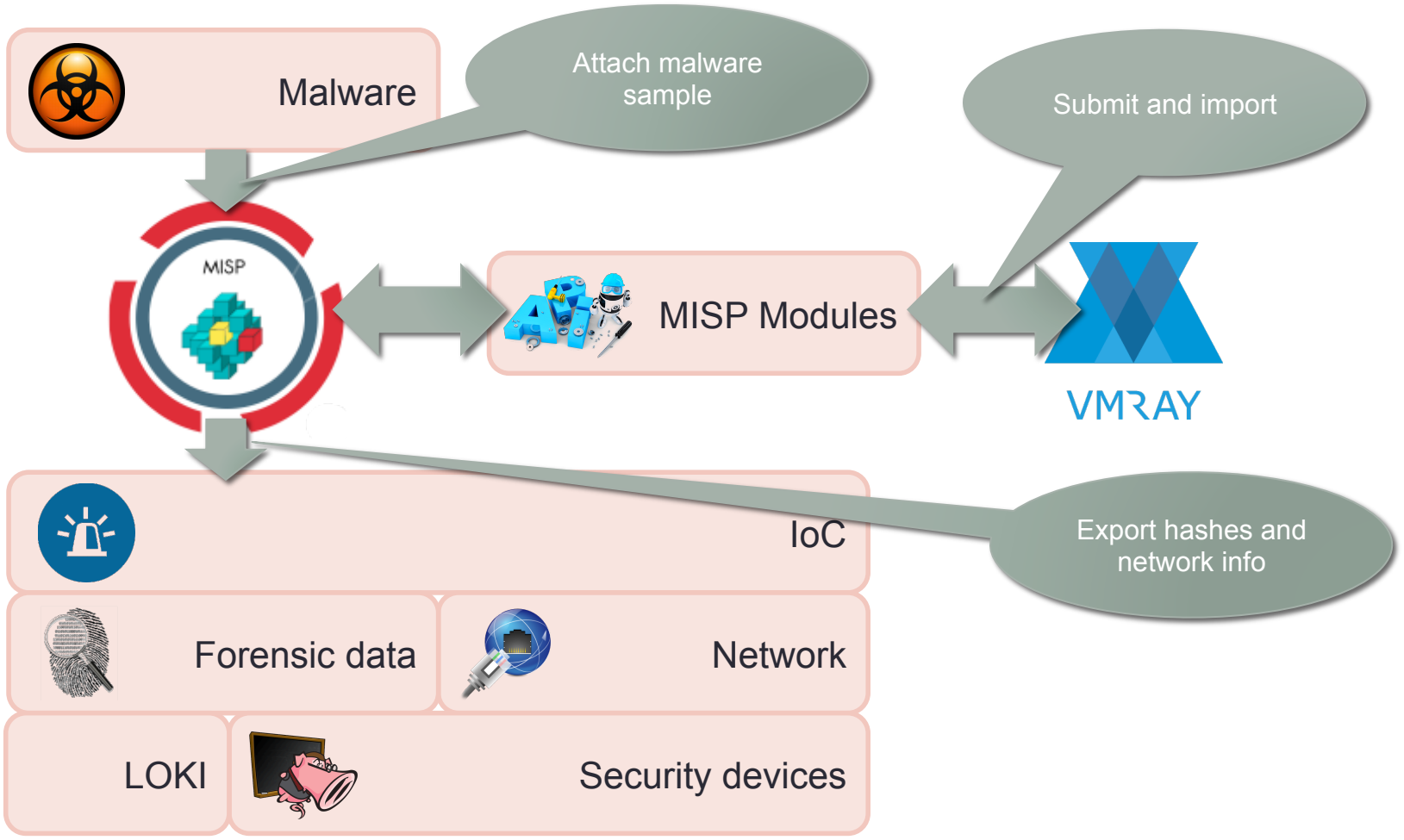


Use Case : E-mail with malware

- We can use **static** analysis
  - limited
  - obfuscated
  - resource intensive

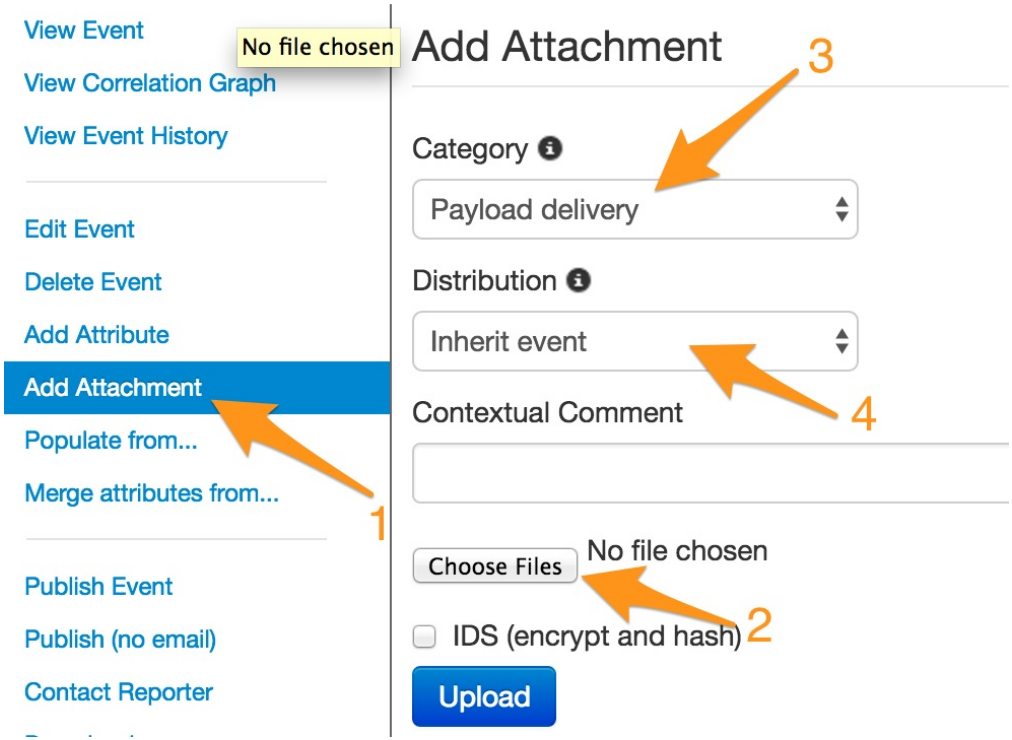
- Use malware sandboxes
  - automated analysis
  - behavior
  - careful with malware that does sandbox evasion / detection

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

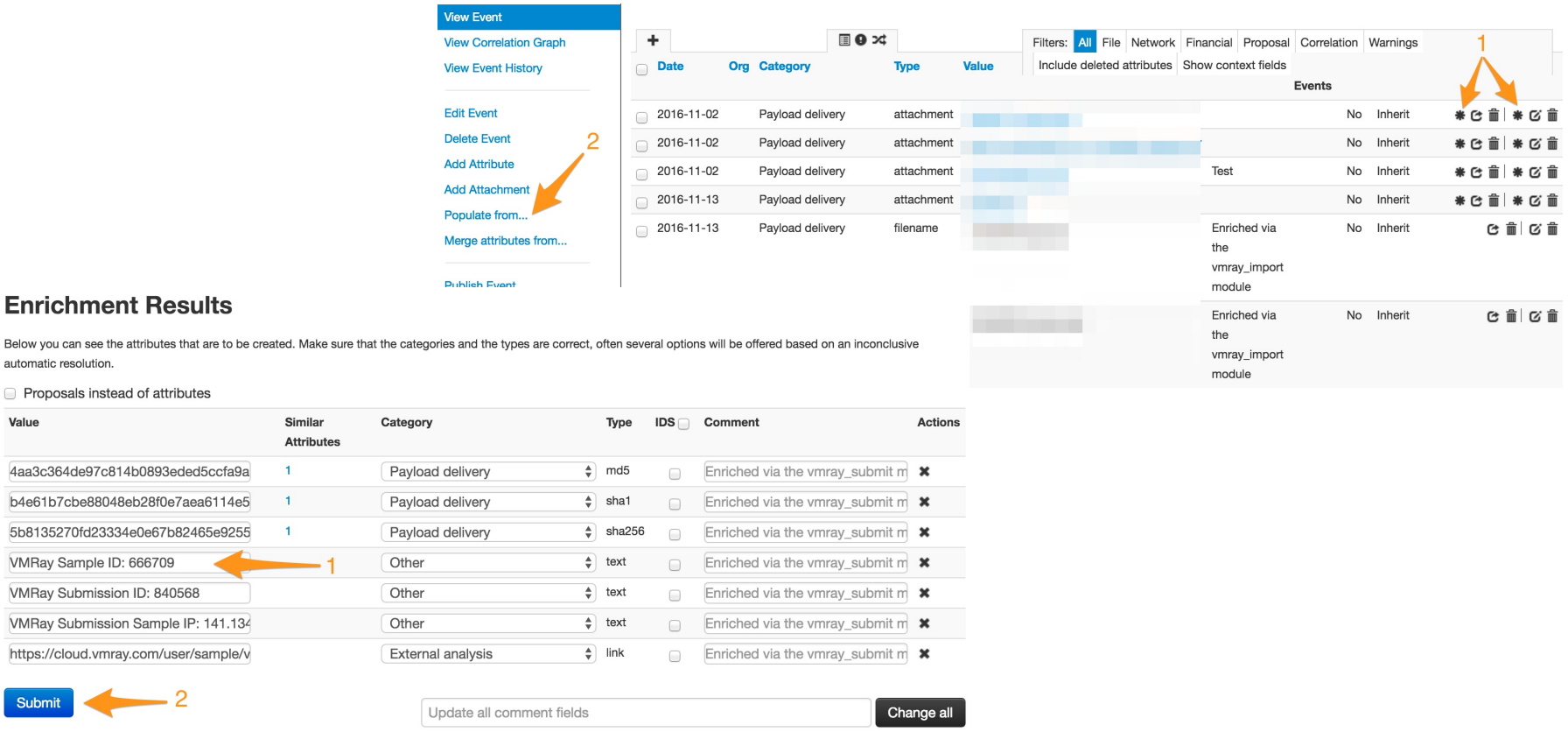


Step 1: Attach malware sample

AddAttachment_orig.mov

Step 2: Submit sample to VMRay

- Via MISP-modules **Enrichment**



Step 2: Submit sample to VMRay

Submit_orig.mov

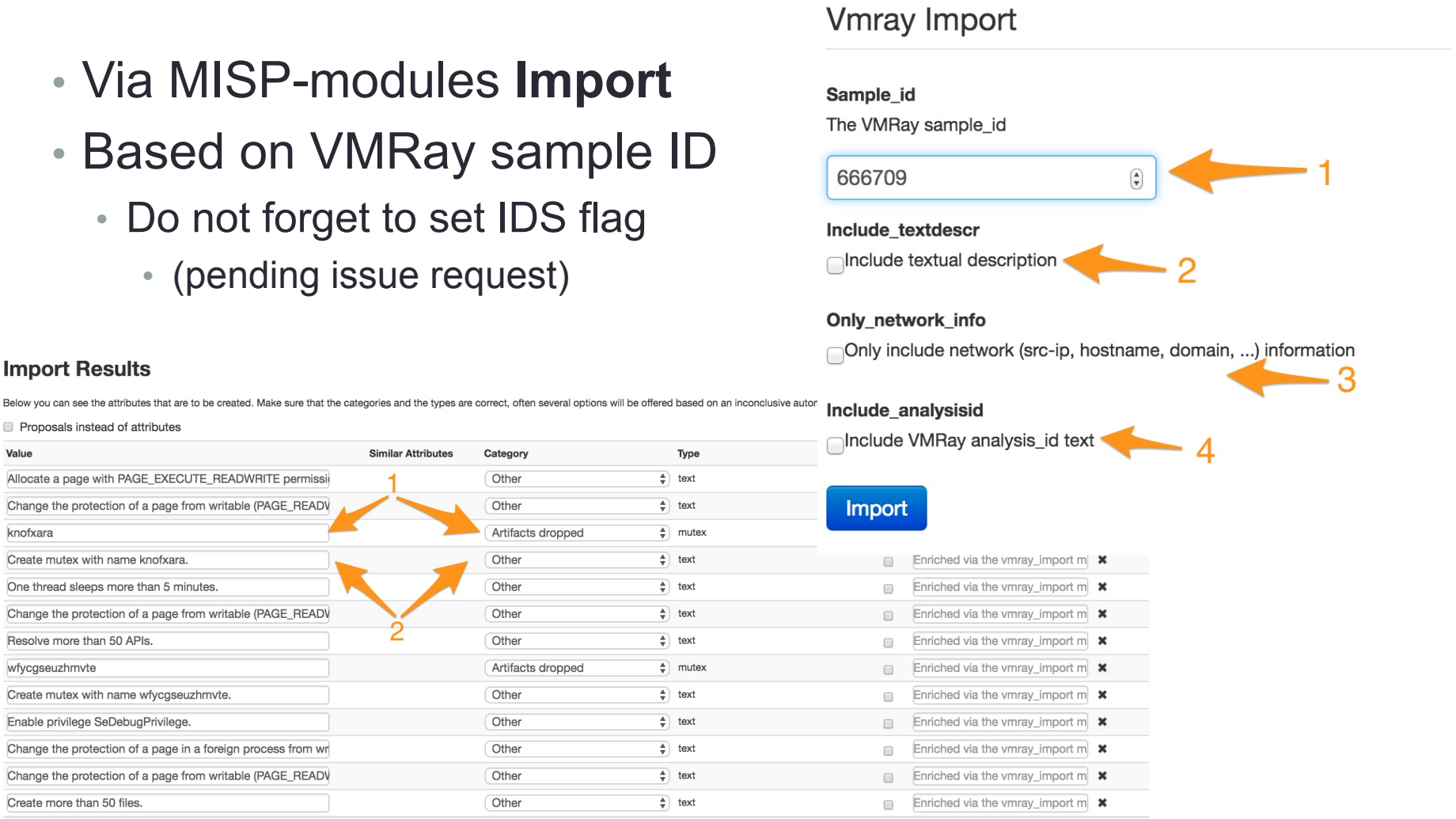
Step 3: Wait for analysis

- 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)



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. 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.	No	N/A	Completed.	Download Generate

- Set of SNORT rules

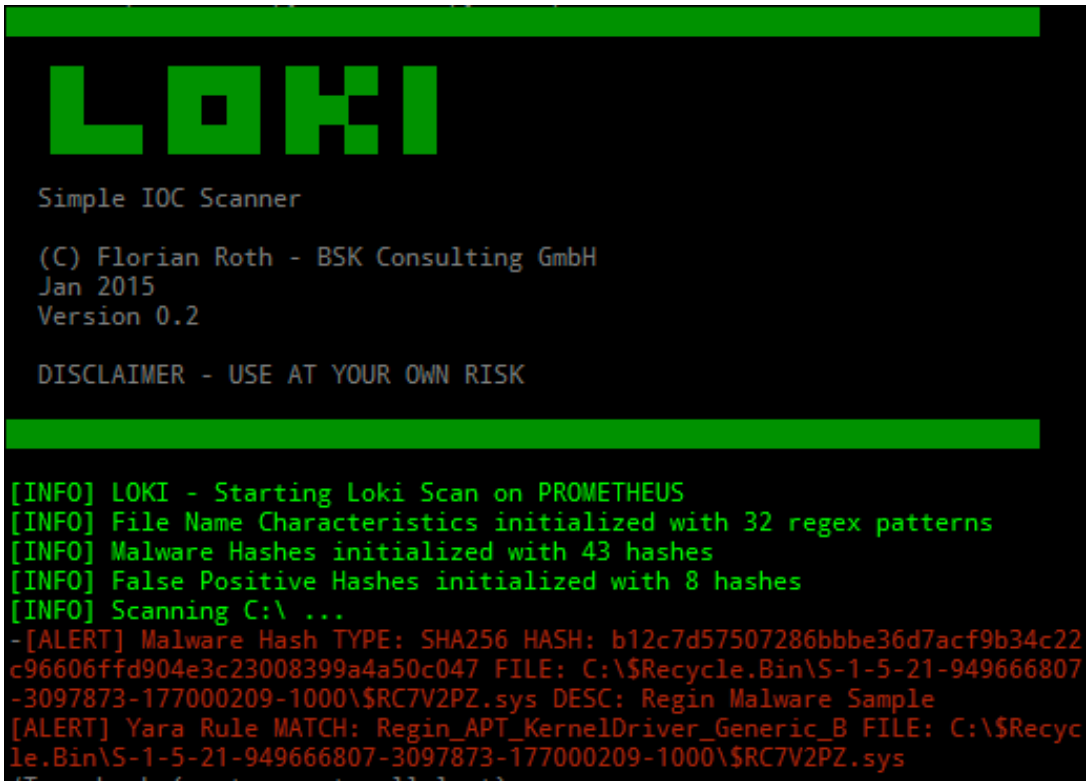
```
alert udp any any -> any 53 (msg: "MISP e2 Domain: dadabada.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|08|dadabada|03|com|00|"; fast_pattern; nocase;  classtype:trojan-activity; sid:4036541; rev:1; priority:3;
reference:url,http://MISP/events/view/2;)
alert tcp 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

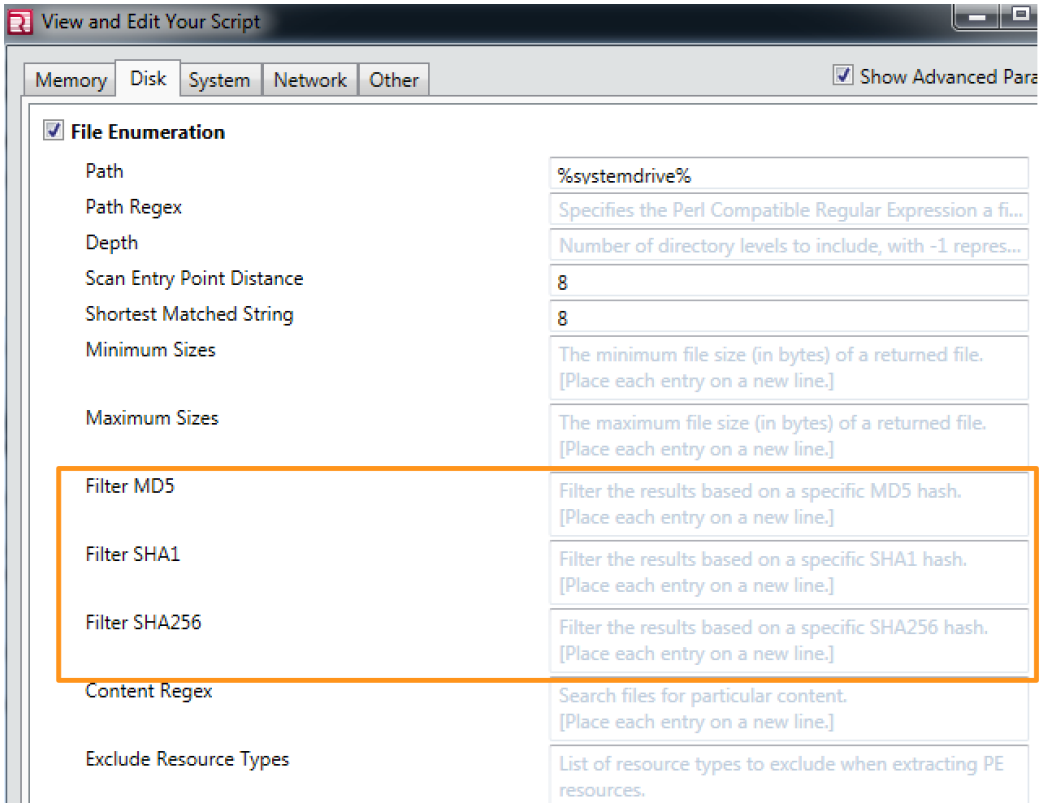
End-point investigation

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



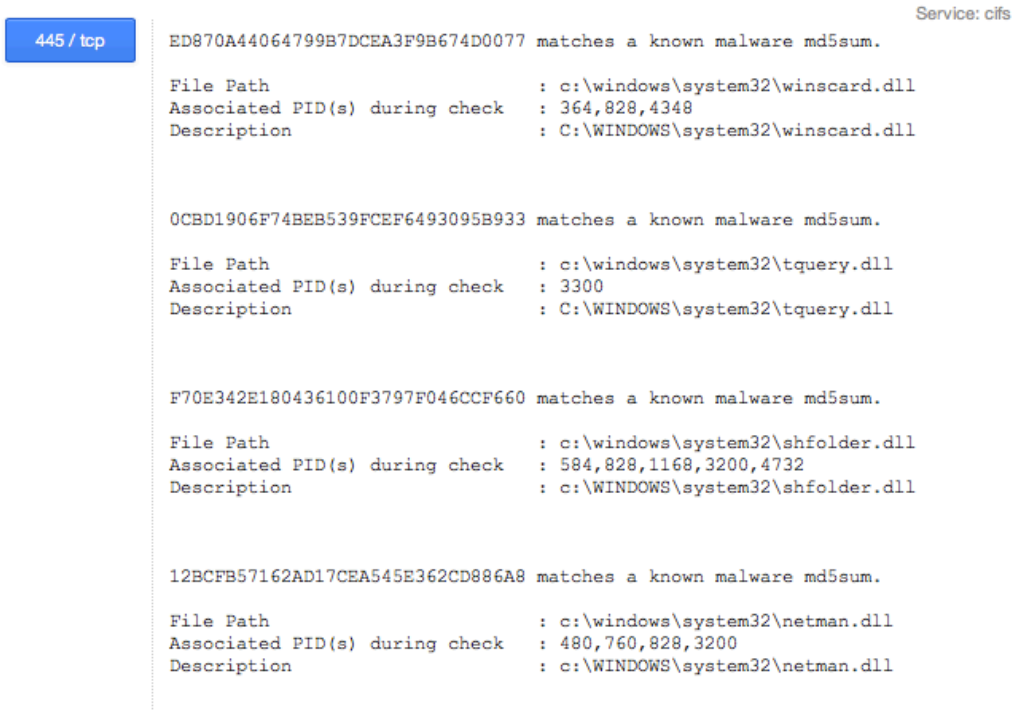
End-point investigation

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



End-point investigation

- Nessus
  - Plugin 65548
    - Search custom file hashes



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