



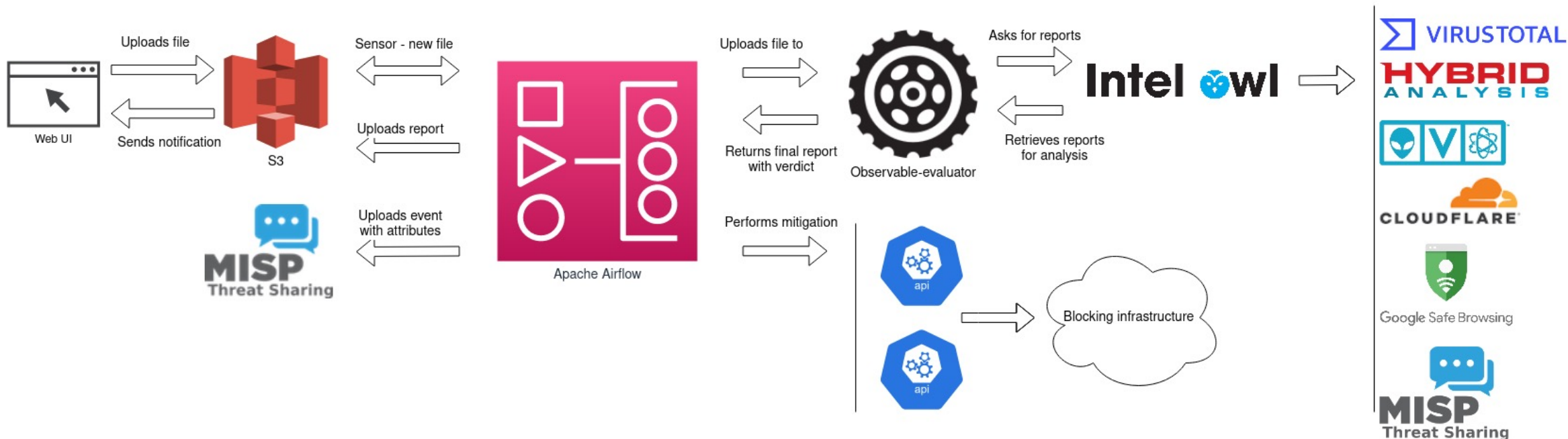
SHARING AND AUTOMATION FOR
PRIVACY PRESERVING ATTACK
NEUTRALIZATION

Malware Analysis Automation Platform

CSIRT-MU, Masaryk University

TLP:WHITE

Malware analysis workflow



1. Provide API keys to supported tools through config file
 - Public API without key may have limited services
2. Run Docker containers
 - Using Docker – `docker-compose up`
 - or Using Vagrant – `vagrant up`



Initial Airflow State

Airflow

DAGsSecurityBrowseAdminDocs

13:51 UTC

AI

DAGs

All 6Active 6Paused 0

Filter DAGs by tag

Search DAGs

DAG	Owner	Runs	Schedule	Last Run	Recent Tasks	Actions	Links
<input checked="" type="checkbox"/> block_multiple_domains	airflow	<div><div></div><div></div><div></div></div>	None		<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	...
<input checked="" type="checkbox"/> block_multiple_emails_dag	airflow	<div><div></div><div></div><div></div></div>	None		<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	...
<input checked="" type="checkbox"/> block_multiple_ips_dag	airflow	<div><div></div><div></div><div></div></div>	None		<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	...
<input checked="" type="checkbox"/> malware_dag	airflow	<div><div></div><div></div><div></div></div>	None		<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	...
<input checked="" type="checkbox"/> malware_starter_dag	airflow	<div><div></div><div>1</div><div></div></div>	*****	1970-01-01, 00:02:00	<div><div>3</div><div>1</div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	...
<input checked="" type="checkbox"/> observable_dag	airflow	<div><div></div><div></div><div></div></div>	None		<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	...

« < 1 > »

Showing 1-6 of 6 DAGs



Malware Gateway

Reports Upload malware

Submit file to malware analyzer

Choose file...



Running Malware Analysis DAG





Report Download

Reports Upload malware

Report is ready

Test malware.docx.exe-report.pdf

Download

New upload



Report for the File

Result

Malware-pipeline evaluated file Test malware.docx.exe as malicious.

Basic information

Name		Test malware.docx.exe
Hash	MD5	8d4b77fa3546149f25bd17357d41fbf0
	SHA1	7289737c1dc462726abbe89335a7702c130bbdcc
	SHA256	bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a
Aliases		myfile
		Andr.PegasusB_Pwk9fuo.apk
		TrojanSpyAndroidPegasus.32507731.apk
		bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a.apk
		bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a
		pegasus.apk
		Andr.PegasusB_6nFFeMO.apk
		6a3efdca-2465-460e-878e-3e6d52790c10
		Andr.PegasusB.apk
		base.apk
		bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a.exe
		pegasus2021_3.apk
Tagged as malicious		HybridAnalysis, OTX Alien Vault, VirusTotal
Tagged as harmless		MISP_Check_Hash

Observables in the Report

Found observables

Observable	Type	Malicious	Detected by	Tagged malicious	Tagged harmless
172.217.194.190	ip	Yes	VirusTotal	OTX Alien Vault	Google Safebrowsing, MISP
142.250.13.188	ip	Yes	VirusTotal	OTX Alien Vault	Google Safebrowsing, MISP
142.250.102.188	ip	Yes	VirusTotal	OTX Alien Vault	Google Safebrowsing, MISP
142.250.27.188	ip	No	VirusTotal		Google Safebrowsing, MISP



MISP Event



View Event

[View Correlation Graph](#)

[View Event History](#)

[Edit Event](#)

[Delete Event](#)

[Add Attribute](#)

[Add Object](#)

[Add Attachment](#)

[Add Event Report](#)

[Populate from...](#)

[Enrich Event](#)

[Merge attributes from...](#)

[Publish Event](#)

[Publish \(no email\)](#)

[Publish event to ZMQ](#)




[Contact Reporter](#)

[Download as...](#)

[List Events](#)

[Add Event](#)

Obtained malware Test malware.docx.exe

Event ID	1
UUID	e83a368e-d954-4472-b7f1-8ea3a0ea9af3  
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Tags	   
Date	2022-01-14
Threat Level	? Undefined
Analysis	Initial
Distribution	This community only   
Info	Obtained malware Test malware.docx.exe
Published	No
#Attributes	11 (1 Object)
First recorded change	2022-01-14 08:43:49
Last change	2022-01-14 08:43:50
Modification map	
Sightings	0 (0) - restricted to own organisation only. 

[-Pivots](#) [-Galaxy](#) [+Event graph](#) [+Event timeline](#) [+Correlation graph](#) [+ATT&CK matrix](#) [+Event reports](#) [-Attributes](#) [-Discussion](#)





MISP Event Cont.

+ [Icons] Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool														
Enter value to search [Search Icon] [Close Icon]														
<input type="checkbox"/> Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity
<input type="checkbox"/> 2022-01-14		Network activity	ip-dst	172.217.194.190	[Globe+] [User+]	[Globe+] [User+]		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
<input type="checkbox"/> 2022-01-14		Network activity	ip-dst	142.250.13.188	[Globe+] [User+]	[Globe+] [User+]		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
<input type="checkbox"/> 2022-01-14		Network activity	ip-dst	142.250.102.188	[Globe+] [User+]	[Globe+] [User+]		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
2022-01-14 Object name: file [Icon] References: 0 [Icon] Inherit [Icon] [Trash]														
<input type="checkbox"/> 2022-01-14		Payload delivery	filename: filename	Test malware.docx.exe	[Globe+] [User+]	[Globe+] [User+]		<input type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
<input type="checkbox"/> 2022-01-14		Other	size-in-bytes: size-in-bytes	1108049	[Globe+] [User+]	[Globe+] [User+]		<input type="checkbox"/>			<input type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
<input type="checkbox"/> 2022-01-14		Other	entropy: float	7.9931541696921	[Globe+] [User+]	[Globe+] [User+]		<input type="checkbox"/>			<input type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
<input type="checkbox"/> 2022-01-14		Payload delivery	md5: md5	8d4b77fa3546149f25bd17357d41fbf0	[Globe+] [User+]	[Globe+] [User+]		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]
<input type="checkbox"/> 2022-01-14		Payload delivery	sha1: sha1	7289737c1dc462726abbe89335a7702c130bbdcc	[Globe+] [User+]	[Globe+] [User+]		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	[Like] [Copy] [Wrench] (0/0/0)	[Comment] [Trash] [Edit]





Malware Analysis Automation Summary

- Platform independent
- One-command deployment
- Speeds-up the initial evaluation of a suspicious file
- Will be released as open-source in April

