Security and Trust in Distributed Systems

Master Degree in New Technologies in Computer Science

2022/23

Open Source Intelligence (OSINT)

Antonio Ruiz Martínez, Pantaleone Nespoli, Félix Gómez Mármol



Outline

Part I

- What's OSINT?
- OSINT Techniques
- OSINT Tools
- OSINT Workflows

Part II

- Maltego
 - Getting started
 - Developing a new transform



https://docs.maltego.com



Home

B+₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩			Maltego Community Edition 4	I.1.15			- = ×	
Investigate View Entities Collections Transfor	ms Machines Collaboration Import	Export Windows					- D	
📗 🕼 🗉 Clear Graph Number of Results 🔍 🗳	🕽 🛛 🙀 🗉 Select All 🛛 🗛 Ad	Id Parents + Add Neighbors A S	Select Children R Select Bookmarked	= Reverse Links S Zoom to Fit S 2	Soom In			
Copy Paste Cut Quick Find	in Entity Select None Ad	Id Children III Add Path 🔅 S	Select Neighbors I Select by Type	Soom 100% S 2	Zoom Out			
× Delete 12 50 256 10k Find File	es Selection > Invert Selection = Ac	ld Similar Siblings A Select Parents 🖉 S	Select Leaves = Select Links	S Zoom to S Z	Zoom Selection			
Home ×								
Start Page Transform Hub								
MALTECO				Transform Hub				
	©Refresh Transform Hub * Update Transforms							
		PATERVA CTAS CE	CaseFile Entities	Cisco Threat Grid	Kaspersky Lab	Shodan	ZETAlytics Massive Passive	
Contraining Education	+	Paterva Paterva	Paterva Paterva	Cisco Threat Grid	Kaspersky Lab	Andrew@Paterva	ZETAlytics	
	·	 Standard Paterva Transforms 	 Additional entities from CaseFile 	• Query Threat Grid's database o	Query Kaspersky Threat Intellig	Query Shodan data from within	Pivots include billions of record	
Currer Doctor		FREE INSTALLED	FREE INSTALLED	PURCHASED SEPARATELT	PORCHASED SEPARATELT	FREE	FREE	
Update 4.1.15 has been released. Find out more here!	Hybrid Analysis	VirusTotal Public API	ThreatMiner		Farsight DNSDB	Blockchain.info (Bitcoin)	SocialLinks CE	
	This set of transforms are base	Query the VirusTotal Public API	Query and pivot on data from T	Query PassiveTotal source and	Query the largest DNS Intellige	For visualizing the Bitcoin block	SocialLinks CE	
	FREE	FREE	FREE	FREE	FREE	FREE	FREE	
	The Movie Database	Have I been Pwned?	People Mon	CipherTrace	FullContact	Clearbit	SocialLinks	
	Paterva	Christian Heinrich	People Mon	CipherTrace	Christian Heinrich	Christian Heinrich	SocialLinks	
	Transforms that visualize the m	Pwned Password v3 Support	Queries peoplemon.com	Cryptocurrency forensics and a	360 insights into the people wh	Enrich sign-ups, identify prospe	Social Networks, Search Engin	
	FREE	FREE	FREE	FREE	FREE	FREE	PURCHASED SEPARATELY	
	Recorded Future Inc.	ThreatConnect	Palo Alto Networks AutoF	ThreatGRID by Malformit	Flashpoint	Intel 471	CrowdStrike Intel	
	· Recorded Future Inc.	ThreatConnect	Palo Alto Networks	Malformity Labs	Flashpoint	MTEL Intel 471	CrowdStrike	
	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	
	CrowdStrike ThreatGraph	SocialNet	Newsl ink	Digital Shadows	MalNet with ProofPoint	Cofense Intelligence	FireEve iSIGHT Intelligence	
	S CrowdStrike	ShadowDragon	Paul@Paterva	Digital Shadows	ShadowDragon	Cofense	FireEye iSIGHT Intelligence	
	CrowdStrike ThreatGraph API T	Social Media Investigative Intell	Transforms for monitoring and	Query the Digital Shadows cyb	Maps malware intelligence. Gr	Search and visualize relationshi	Query FireEye iSIGHT Intelligen	
	PURCHASED SEPARATELY	PURCHASED SEPARATELY	FREE	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	PURCHASED SEPARATELY	
	DomainTools Enterprise	Silobreaker	ZeroFOX Transforms	ThreatCrowd	MaxMind	PhoneSearch	DomainTools Iris	
	DomainTools	Silobreaker	SeroFOX, Inc.	ThreatCrowd	Malformity Labs	PhoneSearch	Domain Tools	
	 Investigate cybercrime with Do PURCHASED SEPARATELY 	PURCHASED SEPARATELY	PURCHASED SEPARATELY	EREE	Query Maxmind Precision Servi PURCHASED SEPARATELY	PURCHASED SEPARATELY	 Investigate and pivot domains, I PLIRCHASED SEPARATELY 	
	FOROTAGED SEPARATELY	TOMOLOGE OF ARMITLE	PONONHOLD OLTANAIELY	1. The last	PONOTHOLD DEPARATELY	FORGERIGED SEPARATELT	PORCHINGED GEFAINATELT	

Transform Hub

- Free and purchased separately sets of transforms
- Some require API key or authentication token to be used



 Create a new Graph (Ctrl+T | Cmd+T)



• Create a new Graph

D+@#80+ # *8	Maltego Community Edition 4.1.15	- = ×
Investigate View Entities Collections Transforms Machines	Collaboration Import Export Windows	•
I Clear Graph Number of Results Q I	Select All Add Parents + Add Neighbors • Select Children Select Bookmarked = Reverse Links Soom to Fit Zoom In	
Copy Paste Cut Quick Find in Entity	Select None = Add Children # Add Path Select Neighbors & Select by Type Soom 100% & Zoom Out	
X Delete 12 50 256 10k Find Files Selection	X Invert Selection Add Similar Siblings A Select Parents Select Leaves Select Links Select Select Leaves Select Links Select Select Leaves Select Links Select Selec	
Entity Palette New Graph (1) *		Overview Machines
Search: Layout		
- Devices		
Desktop Computer		
A personal computer in a form inten		
Device X		
A device such as a phone or camera		
A portable computer suitable for use		<no machine=""></no>
Mobile Phone		
A device which can make and receiv		
5 Smartphone		
A mobile phone that offers more adv		
- Events		
Conversation (Email) A conversation via email		Detail view
Conversation (Phone)		
Incident		
An event or occurrence (for instance		
Manhime (Duninger)		
Run View ×		<no selection=""></no>
		Property View Hub Transform Inputs
<no selection=""> Qutput</no>		
ouput		<u></u>
		<no properties=""></no>

Entity Palette

- Devices
- Events
- Groups
- Infrastructure
- Locations
- Malware
- Penetration Testing
- People
- Personal
- Social Network
- Tracking
- Transportation
- Weapons

E	ntity Palette
Se	earch:
- [Devices
	Desktop Computer A personal computer in a form inter
	Device A device such as a phone or camer
	Mobile Computer A portable computer suitable for us
	Mobile Phone A device which can make and recei
	Smartphone A mobile phone that offers more ad
- 6	Events
X	Conversation (Email) A conversation via email
٩	Conversation (Phone) A telephonic conversation
	Incident An event or occurrence (for instanc
	Meeting (Business) A gathering of people for a commer
	Meeting (Social)

• Add a new Domain entity

🍙 전수공원들인수 한 송명 Maltego Community Edition 4.1.15	
Investigate View Entities Collections Transforms Machines Collaboration Import Export Windows	
🖺 🖺 🗈 Clear Graph Number of Results Q 🔟 🔣 🤋 Select All 🔺 Add Parents 🔸 Add Neighbors 🕫 Select Children 🕷 Select Bookmarked 👘 Reverse Links 🔍	Zoom to Fit 🧟 Zoom In
Copy Paste X Cut Quick Find in Entity Select None Add Children # Add Path Select Neighbors & Select by Type	Zoom 100% 4 Zoom Out
X Delete 12 50 256 10k Files Selection * Invert Selection * Add Similar Siblings A Select Parents # Select Laws * Select Links	Zoom to Selection
Entity Palette Home New Graph (1) *	Overview Machines
Search: a Layout	NOW!
AS An internet Autonomous System (A:	
Banner Freeze	
Domain Name System server name	«Na Machine»
Domain An internet domain	
IPv4 Address paterva.com An IP version 4 address	
ADNS mail exchange record	Detail View
A DNS name server record	Comp Comp
A range of IP version 4 addresses	
An internet Uniform Resource Locat	
Run View	
- Transforms -	
- All Transforms	
To DNS Name (Interesting) [Kobt	
This transform will not he XX rec.	
To DNS Name - NS (name server)	Breach Man
To DNS Name - SOA (Start of Aut 5 + Extracts information for this domai	-Property Very - Properties
To DNS Name - SPF (sender poll) Extracts information for this domai	i type Domain Domain Name paterva.com
To DNS Name (Attempt zone tran	-Graph info
This transform will attempt to perio	Weight
This transform will try to discover v.	Incoming 0
To DNS Name [Robtex]	Outgoing 0 Bookmark
To DNS Name [Using Name Sche	
To Domain [Find other TLDs] This transform will try to find doma	
To Domains (DNS)	

• Modify Domain entity's name to um.es



Run View

- Transforms
 - All transforms having a Domain entity as an Input
- Machines
 - All machines having a Domain entity as an Input
- Also right-click on the entity



Run View Transforms + All Transforms + DNS from Domain 3 + Domain owner detail 34 10 + Email addresses from Domain 3 1 + Files and Documents from Domain * ₩ Machines **Company Stalker** 3 This machine will try to get all email ... **Find Wikipedia Edits** This machine takes a domain and lo... Footprint L1 This performs a level 1 (fast, basic) f... Footprint L2 This performs a level 2 (mild) footpri... Footprint L3 This performs a level 3 (intense) foot ... Footprint XXL This machine is built to work on reall...

Run View	
- • Transforms	H
- All Transforms	H
To DNS Name (interesting) [Robt This transform will search for any	±≊ ⊧
To DNS Name - MX (mail server) This transform will find the MX rec	±≊ ⊧
To DNS Name - NS (name server) This transform will find the NS rec	±≊ ⊧
To DNS Name - SOA (Start of Aut Extracts information for this domai	±≊ ⊧
To DNS Name - SPF (sender poli Extracts information for this domai	±≊ •
To DNS Name [Attempt zone tran This transform will attempt to perfo	±≊ ⊧
To DNS Name [Find common DN This transform will try to discover v	±≊ ⊧
To DNS Name [Robtex] This transform will search for any	★ Si ▶
To DNS Name [Using Name Sche This transform will try test various	<u>†</u> ≦⊧
To Domain [Find other TLDs] This transform will try to find doma	<u>†</u> ≦⊧
To Domains [DNS] This transform extracts all the dom	±₽
To Email address [From whois in This transform obtains whois infor	†≌ ⊧

Run All Transforms





- Play around a bit
 - Add new entities manually
 - Explore entities' properties
 - Run specific transforms
 - Change layout of the graph
 - Save and open a graph
- Create a new entity type
 - University
 - Unique type name
 - es.um.university
 - Category Locations
 - Inherited from Location



	New Entity Wizard (Basic)	
STEPS	BASIC INFORMATION: Enter the details for your new entity below.	1
1. Basic Information	Basic Information	
2. Main	Display name	
Property	(This name will be used in the Entity Palette)	
	Short description	
	(This description will also be showed in the Entity Palette)	
	Unique type name	
	(e.g. paterva.infrastructure.EmailAddress)	
	Category	~
	Inheritance	
	Base Entity	×.
	lcons	
	Large icon (48 x 48) Image Browse Small icon (16 x 16) = Browse	
	Display name is required	
	< Back Next> Finish Ca	ancel



https://docs.maltego.com/support/solutions/articl es/15000015758-writing-transforms



- iTDS (internal Transform Distribution Server) Transforms
 - Web application allowing distribution and management of transforms, seeds and settings
 - Transforms are written as a web services (or application/pages), and the iTDS will call these scripts
 - PROS
 - Once setup transforms are easily distributed to multiple Maltego clients
 - No configuration needed client side, scripts all live in one place
 - Updating instantly impacts all clients
 - Deeper into the protocol (Slider value + Transform settings/Popups)
 - CONS
 - Cannot integrate with applications local to the Maltego client
 - All requests come from a single point (may impact things like rate limiting APIs)
 - Server infrastructure setup is required



Local Transforms

- Pieces of code running on the same machine that the Maltego client application is on
- Very useful for integrating in machine specific tasks
- Written in any language and merely rely on output to be sent via STDOUT
- PROS
 - Machine Specific
 - Nothing ever goes 'over the wire' unless you want it to
 - Simple to write in any language
 - Does not require any server infrastructure setup
- CONS
 - Requires setup on each machine you wish to install them
 - Does not go as deep into the Transform Specification no slider or settings
 - Updating a transform means it needs to be updated on every machine
 - Sensitive data such as usernames and passwords could reside on the computer of the analysts



- Local Transforms
 - Interacted with via STDIN and STDOUT
 - STDIN
 - Entity Value (what is displayed on the graph) \rightarrow this is the first argument.
 - Entity Fields (the fields contained in the entity), separated by #'s and each field is separated name and value by an '=' sign.
 - e.g., "Félix Gómez Mármol" person.fullname=Félix Gómez Mármol#person.firstnames=Félix#person.lastname=Gómez Mármol
 - STDOUT

```
<MaltegoMessage>
<MaltegoTransformResponseMessage>
<Entities>
<Entity Type="maltego.Phrase">
<Value>Hello Félix Gómez Mármol</Value>
<Weight>100</Weight>
</Entity>
</Entities>
<UIMessages>
</UIMessages>
</MaltegoTransformResponseMessage>
</MaltegoMessage>
```