

STRATOSPHERE IPS PROJECT



# ManaTI

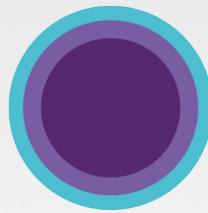
## Web Assistance for the Threat Analyst, supported by Domain Similarity

SEBASTIÁN GARCÍA  
sebastian.garcia@agents.fel.cvut.cz  
@eldracote

RAÚL BENÍTEZ NETTO  
raulbeni@gmail.com  
@Piuliss

Czech Technical University in Prague

<https://github.com/stratosphereips/Manati>

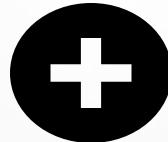


STRATOSPHERE IPS PROJECT

# Stratosphere Project

a free software Intrusion Prevention System

Free protection for NGOs.



Security and Machine  
Learning

Stratosphere Data Analysis Project

**<https://stratosphereips.org/>**



@StratosphereIPS



@stratosphereips

# **What and why?**

ManaTI is a web-based system to analyze, store and organize weblogs faster in a threat analysis team.

# **ManaTI Purpose**

ManaTI assists threat analysis team to  
make their work faster and more  
effective

# Raúl Benítez Netto

- Master Student in CTU
- Member of Stratosphere Project
- Web/App developer focus cyber-security environment
- Photographer aficionado
- raulbeni@gmail.com
-  @Piuliss

# Sebastian García

- Founder of Stratosphere Project
- Creator of Stratosphere IPS
- Researcher on cybersecurity using Machine Learning
- eldraco@gmail.com
-  @eldracote



# Basic knowledge



**Weblogs**



**WHOIS information**



**IoCs (Indicators of Compromise)**

# **Analysis of Malware Behavior in the Network**

The art of understanding the traces of the malware in the network logs.



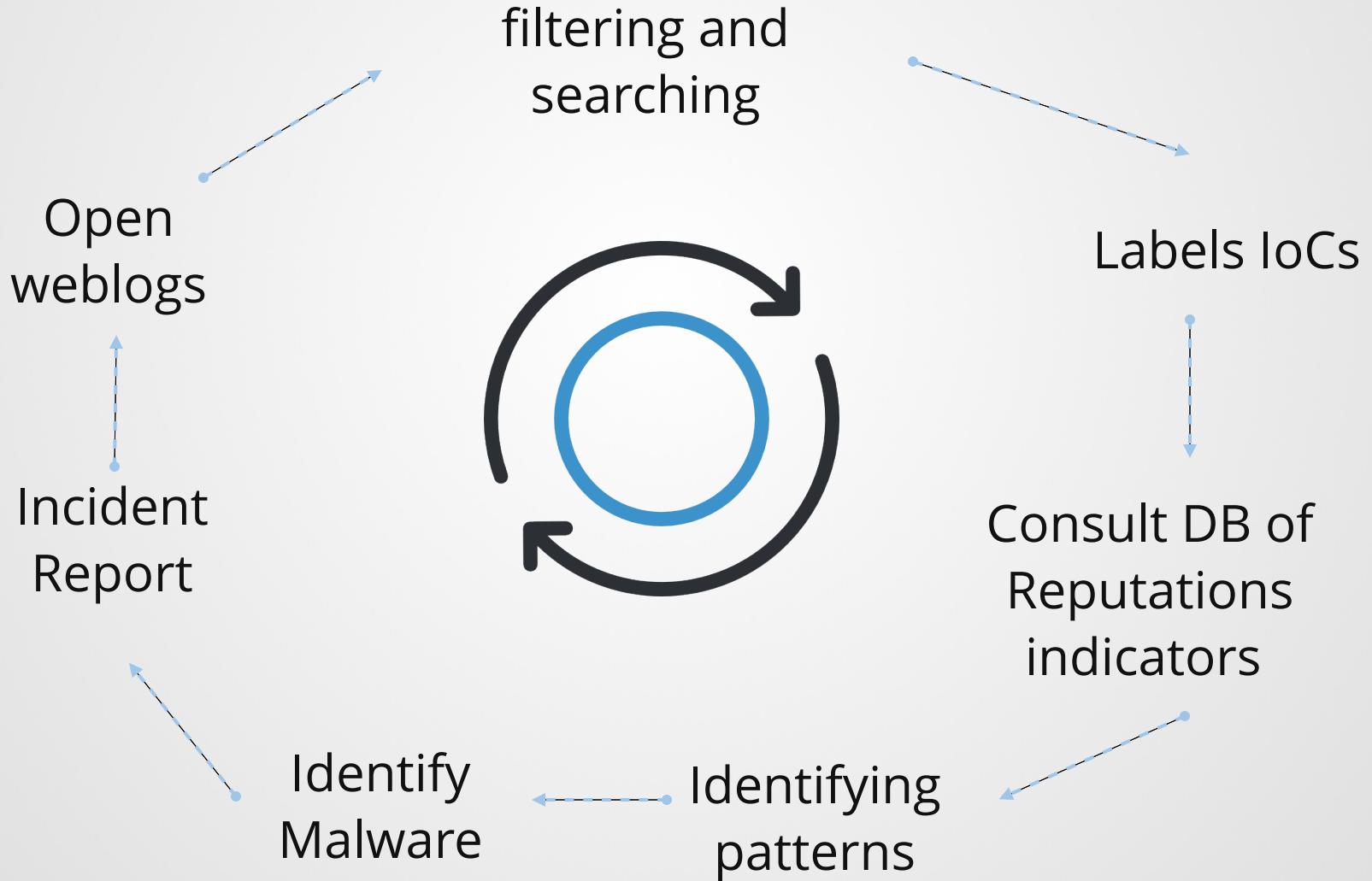
# Malware Traces

Records of connections that malware perform to connect with their C&C



designed by  freepik.com

# Threat Analyst work



# Tools used by Threat Analysts



## Logs Viewer

- Log Parser
- Apache Log Viewer
- LogExpert



## Terminal/Console

- VIM/VI
- WC (Word Count)
- AWK
- GREP



## Big Data analysis

- [splunk.com](http://splunk.com)

# Problems in Threat Analysis



Huge amount of Data



Labeling Data



Repetitive tasks



Much Knowledge lost over time



It is difficult and tiresome

# ManaTI principles

Fast!



Storage



Work in teams

GUI - Web



Provide Assistance

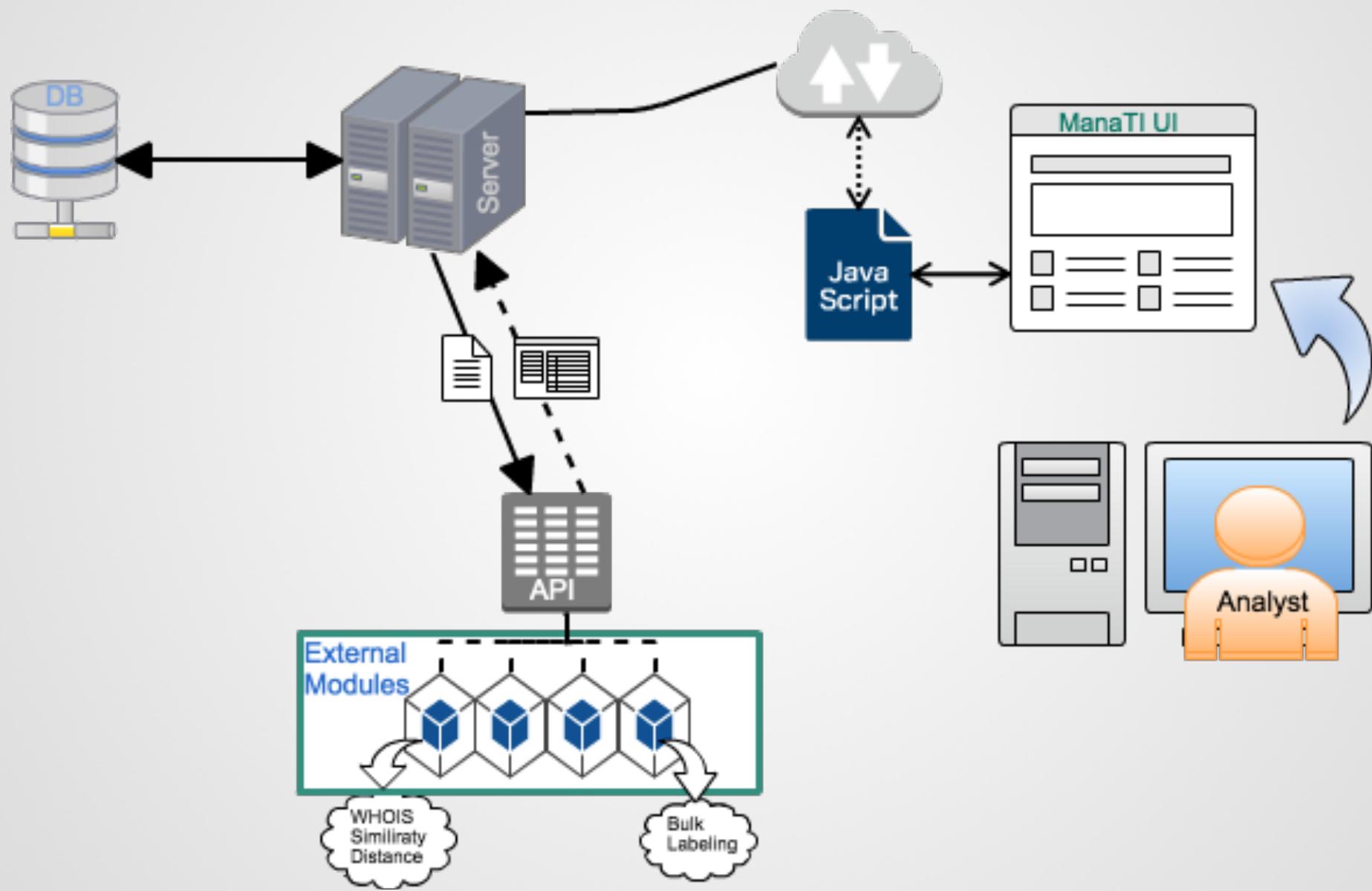
API - Class Interface



Machine Learning  
Algorithm

<https://github.com/stratosphereips/Manati>

# ManaTI Workflow



# **MaNaTI basic features and usability**

# Analysis Sessions and Multi-users

Please Sign In

Please login to see this page. ×

Username

Password

Remember Me

login

# Basic Interface

GUI to vizualise weblogs files.  
Basic table to paginate, filter  
and search weblog data

ManaTI Project  Dashboard  Analysis Session ▼ Version 0.7.0.1 

Analysis Session - http.log (1)  

Home Statistics Section Comments

Search:  Or search by:     
   Page: 1  Previous      ...  

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	trans_depth	method	host	url
210.866612	CnJxvm2YULCJB0UIL	192.168.1.115	49160	67.215.238.66	80	1	GET	download-lb.utorrent.com	/endpoint/hydra-ut/os/win7/track/stabl
212.555548	C69xbD1YhHt2w6Xmt6	192.168.1.115	49161	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
212.560502	Co9n9uk4VSsK3jOEc	192.168.1.115	49162	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
212.821824	COVg4d1VqsRtleh2MI	192.168.1.115	49163	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
213.864970	C07YKn14q29pHlpVWk	192.168.1.115	49158	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
213.865122	CjCXxH2QqeVesprHg2	192.168.1.115	49159	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
231.277311	CuamD31TFvHM2cuSwb	192.168.1.115	49164	45.63.117.51	80	1	GET	ip-api.com	/json?callback=jQuery1910895111848
231.491526	CAK7Phe6gZuLoqiWf	192.168.1.115	49165	67.215.246.203	80	1	GET	update.utorrent.com	/featuredcontent.php?w=6.1
232.290995	CitHyJ1jymoSf5PSti	192.168.1.115	49166	23.21.92.252	80	1	GET	i-50.b-000.xyz.bench.utorrent.com	/e?i=50&e=eyJldmVudE5hbWUiOjoe
249.367892	CFdgUEUZMAiiZvPlD	192.168.1.115	49167	23.21.92.252	80	1	GET	i-50.b-000.xyz.bench.utorrent.com	/e?i=50&e=eyJldmVudE5hbWUiOjoe
249.699403	CJhg3n1bTG9tJ51sKg	192.168.1.115	49168	23.21.92.252	80	1	POST	i-50.b-000.xyz.bench.utorrent.com	/e?i=50
250.247892	CQB4UG2AAzDpEyzra3	192.168.1.115	49169	98.143.146.7	80	1	GET	utorrent.com	/download/langpacks/dl.php?build=42

# Demo Basic Dynamic Table

Please Sign In

Email

Password

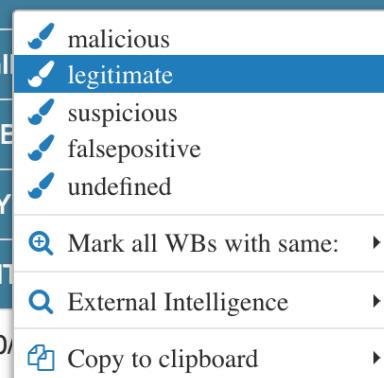
Remember Me



# Weblogs Labelling

It is the basic and more important action for a malware behavior analyst. Detect malicious IoCs

	http.url
38127	http://www.iclnet.org/pub/resources/text/wittenberg/luther/ninetyfive-latin.txt
319444	http://prefaceamachristivocife.com/images/iLw8jg4I/QbbrLage_2FpS4jQxmzE1uQ/LiHd46_2BA/b43LPBQ_2BoED5SEY/HZHsiPqTmGPv/xjRUDKKkp
92009	http://redimcanonesnonsaltemnet.com/1001z.bin
693553	http://prefaceamachristivocife.com/images/xwb2w4tGLGI
697531	http://prefaceamachristivocife.com/images/vAxZMRlx7tvE
.896709	http://prefaceamachristivocife.com/images/c2uLWRTQaY
.946072	http://prefaceamachristivocife.com/images/eiD1X_2FdNIT
.299282	http://prefaceamachristivocife.com/images/gxFj3vbcuap0
.14998	http://prefaceamachristivocife.com/images/dvViz77UlvkW/OrwHsd_2Fl9/68avJmPaDqF73O/KWOPg10l2WEKPGFxqssda/OehRFDKjc2lr4zV/2LWsy
.983652	http://prefaceamachristivocife.com/images/I0i_2F6kDYOENFCwEbCwE/MCrQfCUyrvnuoRWU/5XJ6pkgAZhexFUg/pF_2B9ZQMtpMRLC5FU/RP_2BZ



# Demo - Weblog labeling

Manati Project Welcome, user... (id rev. 451)

Analysis Session - CTU-Malware-Capture-Botnet-35-1.log

Home Statistics Section Comments

Or search by: Page: 1 / 4 Previous Next

ts	id	id.orig_h	id.orig_p	id.resp_h	id.resp_p	trans_depth	method	host	uri	referrer	user_agent
382.174084	C0VnTF12gkqFLDNF7T	10.0.2.107	49159	108.180.117.120	80	1	POST	www.powerontheweb.com	/	-	Mozilla/5.0 (cor
382.190756	Cz2t6v2G720h4K0b0	10.0.2.107	49160	109.234.117.120	80	1	POST	skanner.com.pl	/	-	Mozilla/5.0 (cor
382.276888	CV96UB31Y5gK1a2j0x3	10.0.2.107	49165	185.2.130.120	80	1	POST	areafor.com	/	-	Mozilla/5.0 (cor
382.298497	OxJ0H9R11HOCAUf0o0R	10.0.2.107	49161	74.139.140.120	80	1	POST	zadifirewall.us	/	-	Mozilla/5.0 (cor
382.524348	OrQ3pW3qjXK4Wpmmh4	10.0.2.107	49160	162.159.240.120	80	1	POST	gabtemarina.com	/	-	Mozilla/5.0 (cor
383.155831	CqdW0oOeuKoW5K07B	10.0.2.107	49168	99.192.154.182	80	1	POST	issong-video.com	/	-	Mozilla/5.0 (cor
383.162561	CT95vs2GndKKeuXUai	10.0.2.107	49169	46.105.107.214	80	1	POST	le-manage.com	/	-	Mozilla/5.0 (cor
383.320132	C5d0Sk0emdhEoep59	10.0.2.107	49164	69.67.29.32	80	1	POST	shipitexpress.com	/	-	Mozilla/5.0 (cor
383.339707	CHh6XJ17C8U86d8W02	10.0.2.107	49170	103.28.250.133	80	1	POST	rodeoshow.com.au	/	-	Mozilla/5.0 (cor
383.468086	C457WRH1jEGLW6e5CN5	10.0.2.107	49174	213.186.33.19	80	1	POST	paribet.be	/	-	Mozilla/5.0 (cor
383.542082	COT@W279u486EMvsq	10.0.2.107	49179	149.126.77.703	80	1	GET	www.rodeoshow.com.au	/	-	Mozilla/5.0 (cor
383.641481	CvFlujoquafny27ub	10.0.2.107	49178	184.79.86.115	80	1	POST	www.onli.com	/	-	Mozilla/5.0 (cor
383.729146	Cenad0Gaqy01Quak33	10.0.2.107	49177	12.158.190.246	80	1	POST	mojarer-vacaciones.com	/	-	Mozilla/5.0 (cor

# Exporting Dynamic Table

5769.187006	[REDACTED]
6169.8282	[REDACTED]
6568.989989	[REDACTED]
6968.997117	[REDACTED]
7369.3147	[REDACTED]
7769.437834	[REDACTED]
8169.13947	[REDACTED]
8569.23977	[REDACTED]
8969.28119	[REDACTED]

Show 25 entries

Copy

Excel

CSV

Column visibility

Paint 2

# Comments

001z.bin

/images/xwb2w4tGLGIFObjMhMKy/BSE4TJW5K79QVsPYtZx/ySbmmiK1Xm0atWRSe

g9

Welcome, raul

Add a comment

The domain looks malicious. Reported as been used by a ransomware

OK

Copy to clipboard

Hotkeys List

Session

ump

icious

Prev

BUQYJhy\_2/B6Qs5fEPO2QOzHkCg

# History of changes

User/Module	Previous Verdict	Verdict	When?
raul	malicious	legitimate_malicious	Tue, Aug 22, 2017 12:32 PM
raul	suspicious	malicious	Tue, Aug 22, 2017 12:32 PM
raul	malicious	suspicious	Tue, Aug 22, 2017 12:19 PM
raul	falsepositive_legitimate	malicious	Mon, Aug 21, 2017 6:27 AM
bulk_labeling	falsepositive	falsepositive_legitimate	Mon, Aug 21, 2017 6:21 AM
raul	malicious_legitimate	falsepositive	Mon, Aug 21, 2017 5:57 AM
bulk_labeling	malicious	malicious_legitimate	Mon, Aug 21, 2017 5:57 AM
raul	falsepositive	malicious	Mon, Aug 21, 2017 5:55 AM
raul	legitimate	falsepositive	Mon, Aug 21, 2017 5:27 AM
raul	malicious	legitimate	Mon, Aug 21, 2017 5:27 AM

# Third-party intelligence tools

The threat analysts often use several external services to know about the IoCs

Virus Total Query: prefaceamachristivocife.com

List Attributes	Values										
domain_siblings											
undetected_downloaded_samples	<table border="1"><thead><tr><th>List Attributes</th><th>Values</th></tr></thead><tbody><tr><td>date</td><td>2016-03-26 21:06:26</td></tr><tr><td>positives</td><td>0</td></tr><tr><td>total</td><td>57</td></tr><tr><td>sha256</td><td>259b03ba5daa9e0906782f5ba3b3fabefe06eb25cdca5f58f47fcdd7ba95b9dd</td></tr></tbody></table>	List Attributes	Values	date	2016-03-26 21:06:26	positives	0	total	57	sha256	259b03ba5daa9e0906782f5ba3b3fabefe06eb25cdca5f58f47fcdd7ba95b9dd
List Attributes	Values										
date	2016-03-26 21:06:26										
positives	0										
total	57										
sha256	259b03ba5daa9e0906782f5ba3b3fabefe06eb25cdca5f58f47fcdd7ba95b9dd										
whois	Domain Name: PREFACEAMACHRISTIVOCIFE.COM Registrar: TODAYNIC.COM, INC. Sponsoring Registrar IANA ID: 697 Whois Server: whois.todaynic.com Referral URL: http://www.todaynic.com Name Server: PARK.I-NOW.CN Name Server: PARK.I-NOW.COM Status: clientHold https://icann.org/epp#clientHold Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Updated Date: 24-mar-2017 Creation Date: 23-mar-2016 Expiration Date: 23-mar-2018 Domain name: prefaceamachristivocife.com Registry Domain ID: 2014869364_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.todaynic.com Registrar URL: http://www.now.cn/ Update Date: 2017-03-23T16:00:00Z Creation Date: 2016-03-23T09:37:47Z										

# Statistics and Metrics

See in real time the performance progress of the user

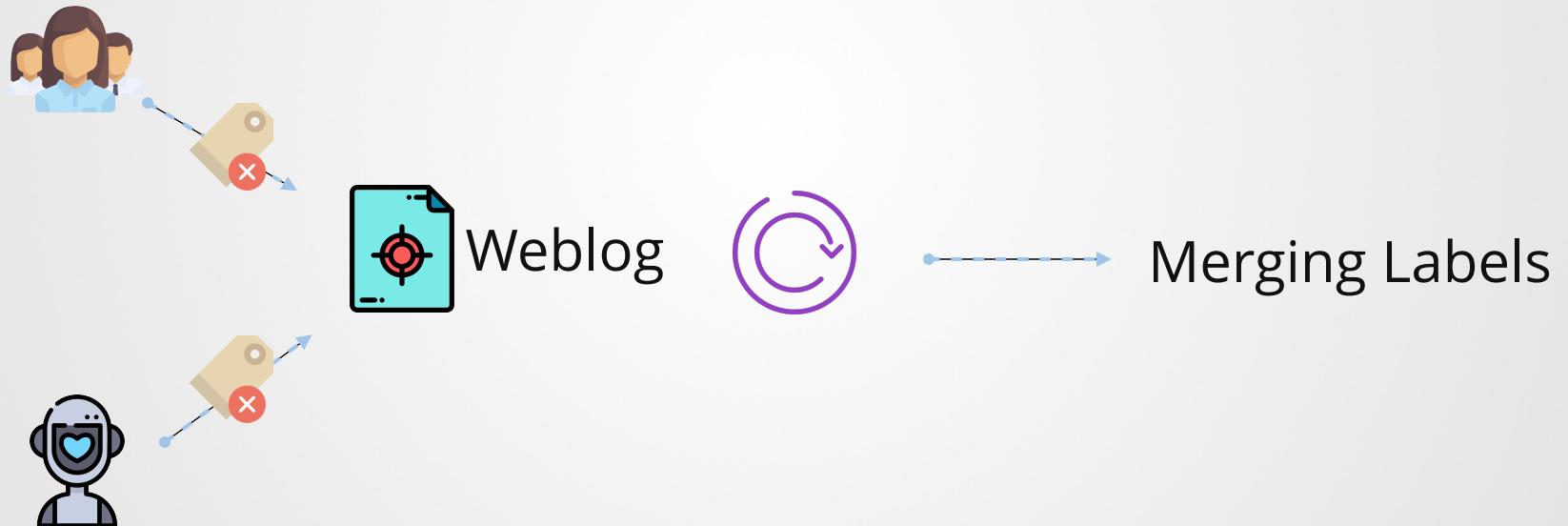


# External Modules

ManaTI allows analysts to create their own scripts and modules to increase the number of labels or weblogs analyzed in a period of time



# Sync with Database - Merging Labels



# WHOIS Similarity Distance Algorithm

How similar are two domains ?

WHOIS fields	Domain A	Domain B	Distance
registrar's name	MARKMONITOR INC.	MARKMONITOR IN	0.0
contact's name.	DNS Admin	Domain Administrator	13.0
org.'s name	Google Inc.	Facebook, Inc.	8.0
contacts emails	dns-admin@google.com	[domain@fb.com]	11.0
zip code	94043	94025	2.0
domain's name	google.com	facebook.com	8.0
duration in days	8401	10229	0.82
servers' name	[ns1.google.com,...]	[a.ns.facebook.com...]	11.0

# WHOIS Similarity Distance Algorithm

List of domains WHOIS related with: prefaceamachristivocife.com ×

WSD Threshold: 75.00

- [assessoriameta.com.br](#)
- [redimcanonesnonsaltemnet.com](#)
- [quodrarusdatmentemplic.com](#)
- [f02783mat0i5r1t.cc](#)
- [siclaicorumunis.com](#)
- [opower.com](#)
- [addthis.com](#)

OK Search Selected

# **WHOIS Similarity Distance Algorithm**



**How to determine if two domains are related?**



**Machine Learning ?**

**<https://github.com/stratosphereips/whois-similarity-distance>**

# ManaTI

# Contributions



All-in-one with Web interface



A scalable and extensible backend server



A novel WHOIS distance measure



Verification of performance improvements

# Future of ManaTI

- Improving WHOIS Similarity Distance
- IOCs labeling
- Import/Export labelled IOCs
- Integration with Stratosphere IPS
- Add more types of files
- Malware Detection
- Active learning
- Community Ideas

# Conclusion

ManaTI :    is a novel tool to facilitate the work  
                  is high functional scalable  
                  user-friendly  
                  can increase the weblogs labelling speed x3.4  
  
                  OpenSource !

# ManaTI Project

Thank you!

SEBASTIÁN GARCÍA

sebastian.garcia@agents.fel.cvut.cz

 @eldracote

RAÚL BENÍTEZ NETTO

benitau@fit.cvut.cz

raulbeni@gmail.com

 @Piuliss



<https://github.com/stratosphereips/Manati>