Tracking Intelligence Project

Angelo Dell'Aera
<a.dellaera@communicationvalley.it>

DIMVA 2009 Rump Session

Tracking Intelligence Project

- TIP is an information gathering framework whose purpose is to autonomously collect Internet threat trends

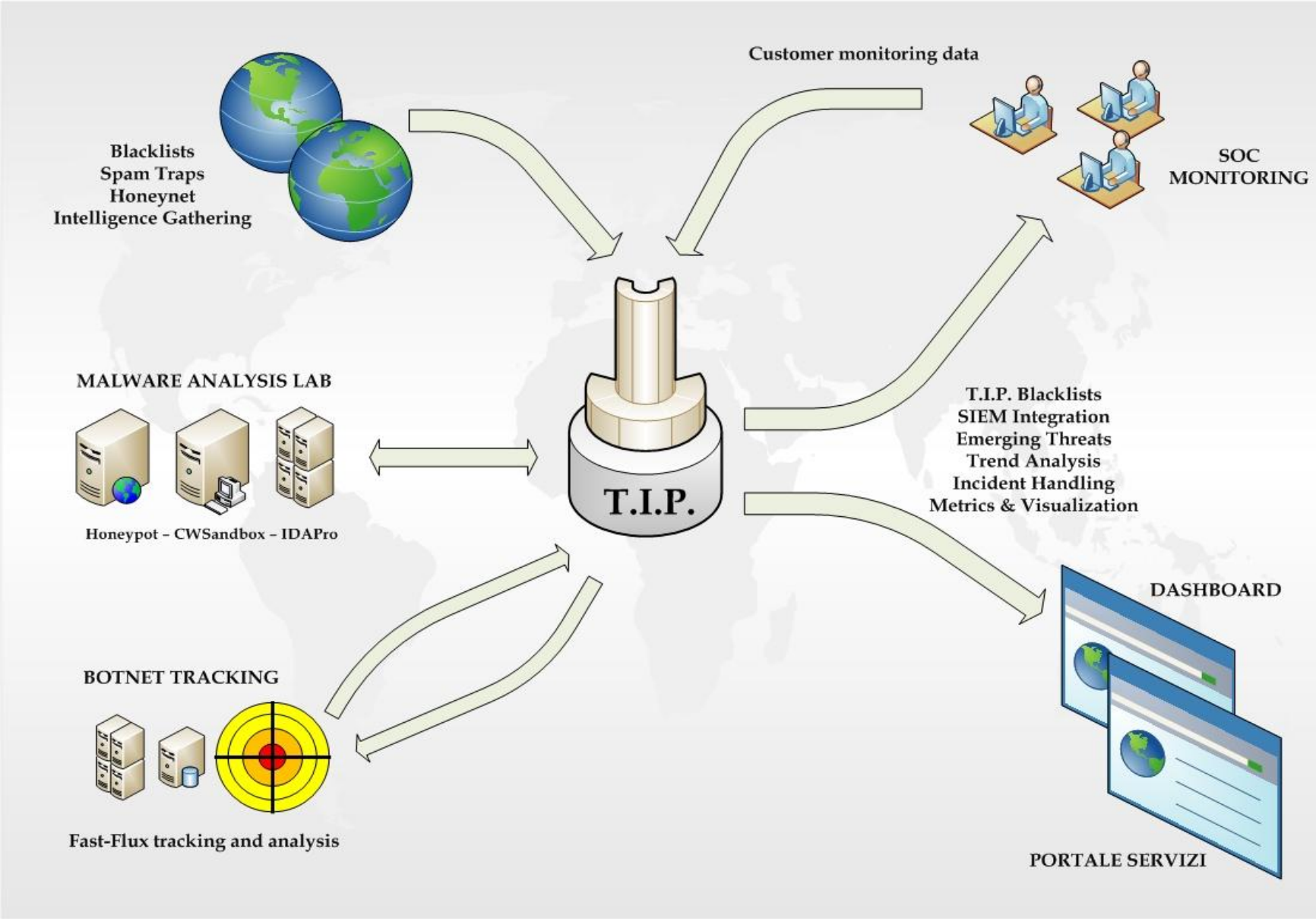
- Entirely written in Python using Twisted and bound to the Django framework in order to abstract the underlying database and to easily build a web interface to the data

Tracking Intelligence Project

- TIP is made up of a few modules which are totally independent one from the other but with each one feeding the other ones

- Its design is based on a core module which acts as a kind of scheduler which schedules what we can call "first level modules" at a precise time in future or in response to a particular event

The Big Picture



Blacklist Module

- Collecting information from sources maintaining domains and network addresses blacklists and weighting these sources with some kind of metrics

- This module acts as a scheduler for submodules, one for each blacklist source

- When the submodule has done its work it notifies the upper scheduler and exits. When all the submodule are done the upper scheduler notifies the core which reschedules the update.

Spamtrap Module

- Currently splitted into two submodules

- The first submodule is scheduled right after the blacklist module and its target are spamtrap repositories which are generally updated daily

Spamtrap Module

- The second submodule is currently under development and its approach is quite different from the first one. Its targets are spamtraps located on mailservers which I administer

- Few of these mailservers generate huge amounts of spam mails and this leads to great performance troubles if you try to download them by POP3/IMAP and then parse

- A different approach was thought for situations like these

Spamtrap Module

- A small agent was developed which has to be run on the mailserver host

- This agent loops listing the spam files in the maildir and parsing them

- When it has done, it saves the interesting data in a serialized form on the filesystem (through the Python cPickle module) and assigns to this data a version number. This allows a remote agent to ask the last version number and download just the missing versions.

Spamtrap Module

- This submodule was developed using Twisted Perspective Broker directly serializing on the wire saved data and currently defines a basic authentication mechanism too

- While developing this submodule I was thinking that it could be nice to use it for sharing data between researchers coming from multiple spamtraps
-
- Suggestions are welcome!

Fast-Flux Module

- This module is mainly based on the metrics defined in the paper "*Measuring and Detecting Fast-Flux Service Networks*" (Thorsten Holz, Christian Gorecki, Konrad Rieck, Felix C. Freiling)

Fast-Flux Module

- The code is written is such a way not to have blocking calls thus realizing a really asynchronous module

- When a domain starts being monitored there's the need to access to backend database thus requiring blocking calls. When this happens, the blocking calls are delegated to the Twisted thread pool with a cloned copy of the collected data in order not to compromise code scalability with not necessary locks

Fast-Flux Module

TIP (Tracking Intelligence Project) BETA

Welcome, **Angelo**. Administration Documentation Change password Log out

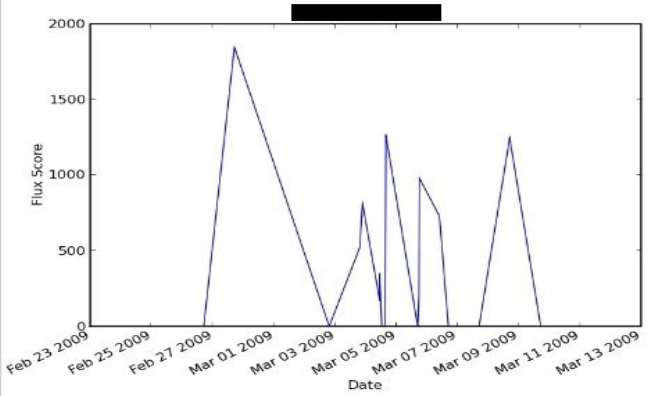
Fast Flux

Fast Flux Domain [redacted]

Domain	Score	Hosts	ASNs	First seen	Last seen
[redacted]	2552.7	431	107	2009-02-27 17:27:03.573844	2009-03-09 17:15:39.087170

FastFlux Score Graph

[redacted]



FastFlux A

IP Address	Hostname	ASN	Country	First seen	Last seen
[redacted]	[redacted]	3209 (ARCOR-AS Arcor IP-Network)		2009-03-08 20:30:34.879104	2009-03-09 17:16:03.219094
[redacted]	[redacted]	7132 (SBIS-AS - AT&T Internet Services)		2009-03-08 21:01:47.451310	2009-03-09 17:16:03.188412
[redacted]		34977 (PROCONO-AS PROCONO S.A.)		2009-03-08 17:26:40.921340	2009-03-09 17:16:03.168379
[redacted]	[redacted]	8551 (BEZEQ-INTERNATIONAL-AS Bezeqint Internet Backbone)		2009-03-09 12:40:45.923099	2009-03-09 17:16:03.139758
[redacted]	[redacted]	16338 (AUNA_TELECOM-AS Cableuropa - ONO)		2009-02-27 19:39:17.472518	2009-03-09 17:16:03.103352
[redacted]		31499 (YCC-AS Ekaterinburg-2000 LLC)		2009-03-09 16:46:08.905731	2009-03-09 16:46:08.905790

Search

Domain

IP Address

Future Work

- Incrementing the number (and types) of information sources
- Including a client honeypot
- Develop a system for automatically generate blacklists
- Last but not the least release TIP as a GPL code as soon as it will meet the quality requirements I would like to reach so stay tuned!

Additional References

- Angelo Dell'Aera Technical Blog
- http://buffer.antifork.org/wordpress