Using MISP & PyMISP to create solutions - WORKSHOP (3 Hours)

(Hackfest.ca November 2018)

David Girard, Sr. Security Researcher

Disclaimer

The views presented are those of the speaker and do not necessarily represent the views of Trend Micro Inc, or its components.

Les opinions présentés ici sont celles du conférencier et ne représente pas nécessairement celles de Trend Micro Inc, ou de l'une de ses composantes.

Trend Micro is not responsible for anything he says. We barely know him.

TREND MICRO

Prerequisites

- Know basic Python or any programming? Do you?
- Python 3.5+ for PyMISP but we only tested 3.6 on Windows and Ubuntu. Mac should work
- Use the recommended Wi-Fi so you get access to AWS MISP we provide you
- Virtual Box or Vmware to run VM
- Less than 4 GB of RAM to run Python and VM but we recommend 8GB with PyCharm (it use JAVA)!
- 12 GB of Disk for VM. 15 recommended.
  - 2.3 GB image, 7.8 GB imported, Python + Pycharm…processing

Workshop Agenda

1. Goal
2. Logistics & Lab
    1. Start Installation of the workshop prerequisite
3. Quick intro to MISP
4. PyMISP Overview
5. Let's code
    1. Lab overview
    2. Exercises
6. Conclusion

Basic Python Skills Required!

1. Goal

- The goal of this workshop is to introduce you to MISP and PyMISP to help you develop Threat Intelligence solutions for research or to help customers and partners.
- While our product use STIX/TAXII, you may need a TIP (Threat Intelligence Platform) as a repository. MISP is a popular Open Source with a rich ecosystem. MISP is compatible with STIX/TAXII.

Notes

- You may use or create MISP integrations with our research systems, our products or 3rd parties.
  - Check on internal wiki for a list of integrations and internal API to SPN
  - In some cases, others solutions might better fit. So if you need some graph analysis, use ArangoDB or StarDog.
  - Elastic, Pandas, BeautifulSoup, Tensorflow…are common.
  - For intelligence gathering we use many libraries, you may also look at Harpoon and Hyppocampe
    - https://github.com/Te-k/harpoon
    - https://github.com/TheHive-Project/Hippocampe (elastic friendly)

References

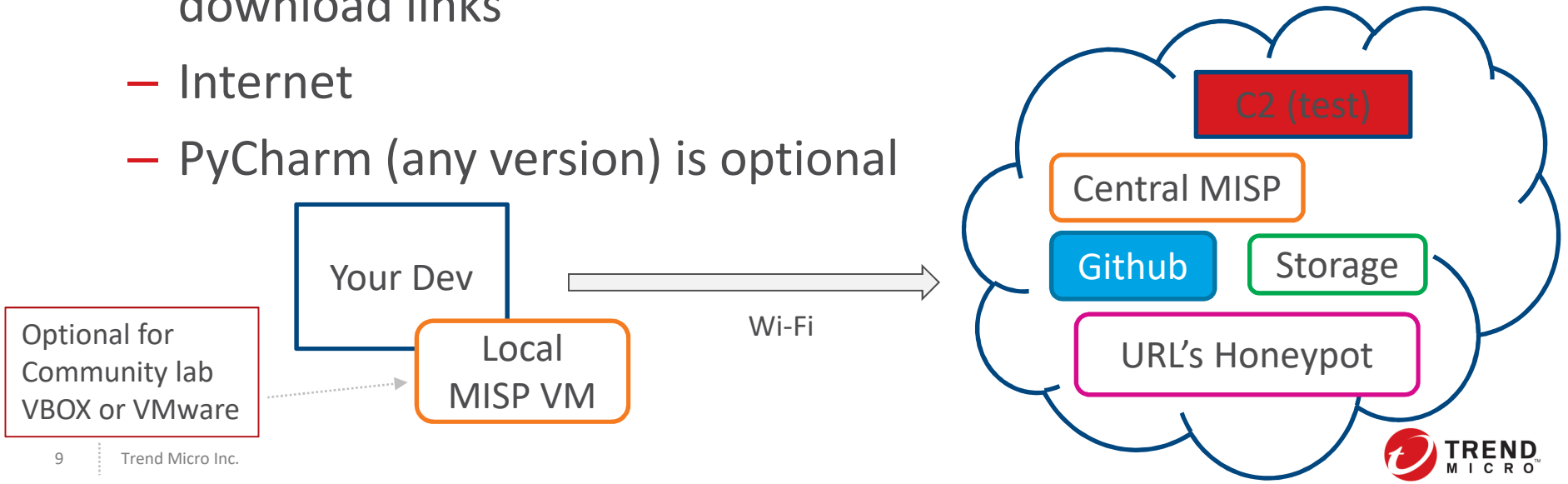
- If you need more informations on MISP they have training material at :
  - https://www.circl.lu/services/misp-training-materials/
- And a lot of code samples in their github
  - https://github.com/MISP/MISP

We encourage you to get trained if you need to develop MISP solutions. Check with CIRCL or ask a MISP SME internally

2. Logistics & Lab

- Your Dev Env
  - Windows/Linux with Python 3.5 + (3.6 used)
  - Come and get a sheet for your API Keys and download links
  - Internet
  - PyCharm (any version) is optional

Mac may work
But not tested



Environment (no more than 30 min I hope ☺)

1. Github to clone 1st: https://github.com/girdav01/misp-workshop
2. Local MISP v2.96, VMWare or Vbox VM on 10 UBS or download from : https://www.circl.lu/misp-images/latest/ 2.1 GB over wifi!
    1. Pass them around quickly! We need to get started. But we use AWS in first exercise
    2. I need the stick back for other workshops!
3. Install Python 3.6 environment + PyMISP (pip3 install pymisp)
    1. We use PyCharm optionally. Use your favorite IDE.
4. Wifi : Use the workshop wifi so you can access AWS. Only this network is white listed on port 443
5. Central MISP in AWS : https://ec2-54-157-205-95.compute-1.amazonaws.com (This AWS instance will be shut down after the Workshop)
    1. Come in front to get an API Key & trainee email. Got 60 of them. Password will be : HackFestDecade!

Python 3.6+

- Get Python from : https://www.python.org/downloads/
  - Use 64 bits for your OS
- PyCharm (any Edition) is ok. If you are full time developper you may need Pro. But CE works fine
  - https://www.jetbrains.com/pycharm/
- Install PyMISP (pip3 install pymisp)
- Clone the workshop github and open it

3. Quick Intro to MISP

http://www.misp-project.org

- The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators.
- A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.
- In 2011, a Belgium Defense employee (Christophe Vandeplas) start working on a prototype after being frustrated to share intelligence through email. In 2012, NATO heard about it
- After that, other organizations started to adopt the software and promoted it around the CERT world. (CERT-EU, CIRCL, and many others …)
- Trend Micro : different projects and some researchers use it

TREND MICRO

MISP concepts

- Events, Attributes, Tags, Taxonomies
- Objects, References,Galaxies, Sightings…
- Feeds, Organizations, Warninglists…

- See updated feature list here:
  - https://www.misp-project.org/features.html

MISP Events - Examples from DDI script

APT - SIMBOT - HTTP (Request)

DDI generated

MISP generated

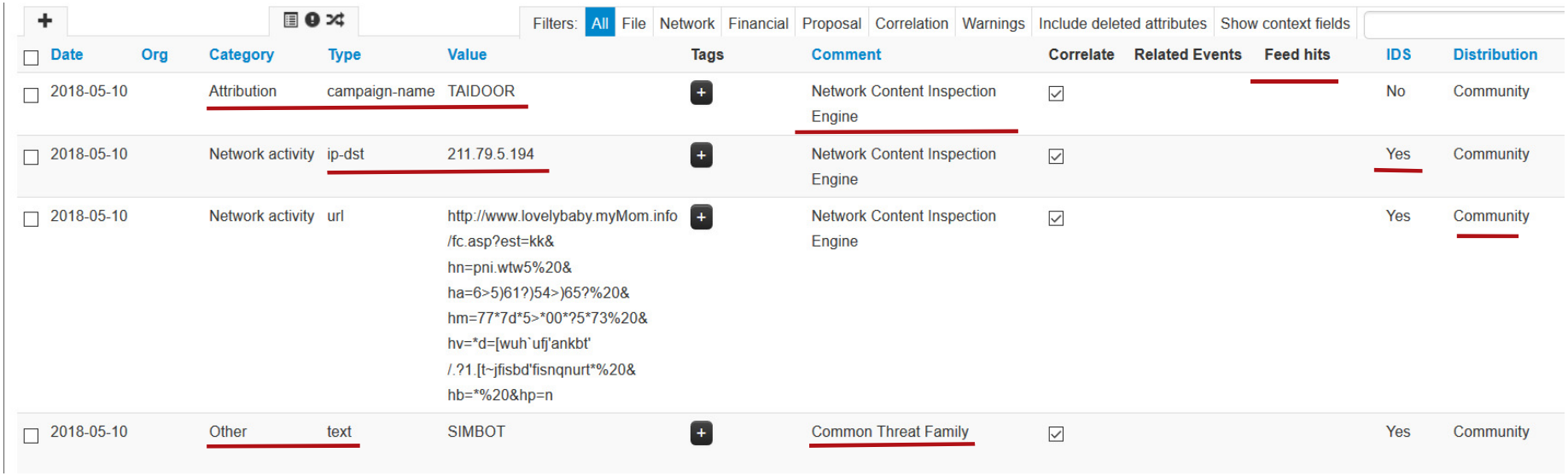
Configured by customer

Generated by script

Event ID	1634
Uuid	5af3a8d9-3f68-4103-8652-0eaec0a82c81
Org	CTX2
Owner org	CTX2
Contributors	
Email	david_girard@trendmicro.com
Tags	Command and Control Communication x tlp:green x Threat Source: Trend Micro Deep Discovery x APT x +
Date	2018-05-10
Threat Level	High
Analysis	Completed
Distribution	This community only
Info	APT - SIMBOT - HTTP (Request)
Published	Yes
#Attributes	4
Sightings	0 (0) - restricted to own organisation only.
Activity	

TREND MICRO

MISP Event Attributes (1)



Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
2018-05-10		Attribution	campaign-name	TAIDOOR		Network Content Inspection Engine	☑			No	Community
2018-05-10		Network activity	ip-dst	211.79.5.194		Network Content Inspection Engine	☑			Yes	Community
2018-05-10		Network activity	url	http://www.lovelybaby.myMom.info /fc.asp?est=kk& hn=pni.wtw5%20& ha=6>5)61?)54>)65?%20& hm=77*7d*5>*00*?5*73%20& hv=*d=[wuh`ufj'ankbt' /.?1.[t~jfisbd'fisnqnurt*%20& hb=*%20&hp=n		Network Content Inspection Engine	☑			Yes	Community
2018-05-10		Other	text	SIMBOT		Common Threat Family	☑			Yes	Community

We don’t have a feed hits in this screen shot but if another OSINT Threat Intelligence would have a hit then it would appear. On a hit, you click on the hyperlink and you get to the feed that could be AlienVault OTX for example that reported that SHA1. IDS to Yes mean it can generate IDS Snort or Bro rules.

TREND MICRO

MISP Event Attributes (2)

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
2018-05-10		Antivirus detection	text	JS_NEMUCOD.SMPOW3		Advanced Threat Scan Engine	☑	1310
2018-05-10		Network activity	url	http://hnwpquyu.datethebest。ru/f/sfskw/?photoid=Abigale		Advanced Threat Scan Engine	☑	
2018-05-10		Payload delivery	sha1	741ea9fca395db08091a33663e3147a66ec17a58		No Report	☑	
2018-05-10		Payload delivery	sha256	58fca5840eb68a4265d26c23dc11e44c4ad8689fa61da27d4cba01ac403f75ed		No Report	☑	
2018-05-10		Payload delivery	malware-type	Trojan		SMTP	☑	1093 1097 1102 1114 Show Show

Lateral movement case

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
2018-05-01		Network activity	text	SMB		Network Content Inspection Engine	☑	1462 1518 1546 1547 Show Show 71more...
2018-05-01		Payload delivery	text	MS17-010		Exploit Generic SMB	☑	1397 1464 1466 1468

MISP Event Attributes (3)

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
2018-05-01		Network activity	url	http://192.168.220.137 /foxit_reader_plugin_url_bof__generic_shell_reverse_tcp__no_evasion__jmp_call_additive.pdf?%70%66%62%46%4b%59%73%6a%45%43%44%47%4d%54%6b%46%75%4f%6d%4b%73%4e%43%49%6d%4e%46%46%53%77%53%42%62%7a%6d%5a%55%4d%42%45%54%68%43%62%56%6e%65%61%7a%6e%42%4e%73%6b%72%43%4f%4d%78%4c%77%65%42%64%5a%52%46%56%42%55%77%6b%49%65%64%54%57%77%4d%4e%43%75%75%54%5a	+	Network Content Inspection Engine	☑	1461 1487 1533 1544
2018-05-01		Other	text	METASPLOIT	+	Common Threat Family	☑	1487 1533 1544
2018-05-01		Payload delivery	text	OSVDB-89030 - Foxit Reader Plugin for Firefox URL String Stack Buffer Overflow	+	Exploit Browser HTTP	☑	1461 1487 1533 1544

Date	Org	Category	Type	Value	Tags	Comment
2018-05-01		Payload delivery	vulnerability	CVE-2017-3040	+	Exploit Generic
2018-05-01		Payload delivery	text	MS17-010	+	Exploit Generic

If a CVE number is present, we can use vulnerability type, otherwise we use text or try the vulnerability object

TREND MICRO

MISP tour

4. PyMISP

- Go through library in github

Configure your local MISP

- Default credentials for Web and CLI are:
  - Login to CLI (misp:Password1234) and get your IP
    - It is DHCP by default. If you want a fix just change it, it is an Ubuntu 18.04 so it should be easy
  - In your host file add an entry misp.local
- At first Web login you must change the password, use HackFestDecade!
  - Default is admin@admin.test:admin

Configure your local MISP (2)

- Setup URL
- Create Organization (use your number that come with API Key)
  - hackfest03
- Create a sync user
- Create a publisher account and take note of your API

5. Let's code (2 approches pure API or JSON)

1. Hello MIPS
2. Retreive IoC's & Create Events/Attributes
3. Search MISP for existing attributes
4. Use MISP to convert intelligence into other formats
    1. STIX, Snort rules, OpenIoC, Yara
5. Exploit & Malware Screen Scrapping Example (demo)
6. Turn a product Dark Data into Threat Intelligence (demo)
7. Create a community between your local MISP and the Central MISP – we may not have time for this one

Show some real examples

- Exploit & Malware Screen Scrapping Example
- Turn a product Dark Data into Threat Intelligence

6. Conclusion

- MISP got a rich API with PyMISP and many extensions. This makes it an amazing tool to create solutions. Go take advantage of it!

- Questions?
- Merci, Thank you

Additional informations

Change MISP IP to static

sudo nano /etc/netplan/50-cloud-init.yaml

```
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    ens33:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.44.100/24]
      gateway4: 192.168.44.2
      nameservers:
        addresses: [192.168.44.2,8.8.8.8]
```

To apply the changes, run:
sudo netplan apply

Synchronization Example

- Central MISP with Local MISP collecting
- Add Central Server to Local MISP
- Create Push and Pull rules
- Test

- David_girard@trendmicro.com

MISP additional cron settings

Since synchronization might crash easily, we recommend to handle it with Cron jobs. Problem in version 2.9x. Check MISP blog if any solution exist.

add to /etc/cron.d/misp

```
#  /etc/cron.d/misp-feeds
#  This will force misp pull and push sync actions every 15 minutes using the default user on the default instance id
# format /var/www/MISP/app/Console/cake server <pull/push> <userid> <serverid> <kwargs>
#
*/15 * * * *    www-data    /var/www/MISP/app/Console/cake server pull 1 1 update
*/15 * * * *    www-data    /var/www/MISP/app/Console/cake server push 1 1
```

(edited)

edit /etc/php/7.2/apache2/php.ini and in the [Session] section set session.save_handler and session.save_path to the following:

```
[Session]
; Handler used to store/retrieve data.
; http://php.net/session.save-handler
session.save_handler = redis

session.save_path = tcp://localhost:6379
```