

MISP Workbench - Manage your very own Cyber Threat Intelligence tool

MISP - Malware Information Sharing Platform & Threat Sharing



CIRCL
Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:WHITE*

September 4, 2016

Functionalities of MISP Workbench

- **Merging** of events (campaign, attacker, tool, victim, ...)
- **Comparing campaigns** composed of multiple events
- **Expanding** MISP in a timely manner (no Apache, MySQL & PHP)
- Extraction of **PE indicators** & correlation
- Reduce an investigation on a **subset of events**
- **Very fast lookups**, use the dataset in an **untrusted environment**

MISP Galaxy

- List of known keywords:
 - Adversary groups (with synonyms)
 - Threat actors tools (with synonyms)
- Used to automatically group related events

MISP galaxy - elements of threat actors

- An element list of threat actors included by default.

```
1 {
2   "synonyms": [
3     "PLA Unit 61486", "APT 2", "Group 36",
4     "APT-2", "MSUpdater", "4HCrew", "SULPHUR"
5   ],
6   "country": "CN",
7   "refs": [
8     "http://cdn0.vox-cdn.com/assets/4589853/
9     crowdstrike-intelligence-report-putter-panda.
10    original.pdf"
11  ],
12  "description": "The CrowdStrike Intelligence team has
13    been tracking this particular unit since 2012, under
14    the codename PUTTER PANDA, and has documented activity
15    dating back to 2007. The report identifies Chen Ping,
16    aka cpyy, and the primary location of Unit 61486.",
17  "group": "Putter Panda"
18 }
```

MISP galaxy - elements of threat actors tools

- An element list of tools used by various threat actors.
- The key-values can be freely combined.

```
1 {
2   "value": "MSUpdater"
3 },
4 {
5   "value": "Poison Ivy",
6   "description": "Poison Ivy is a RAT which was freely
7     available and first released in 2005.",
8   "refs": ["https://www.fireeye.com/content/dam/fireeye-
9     www/global/en/current-threats/pdfs/rpt-poison-ivy.
10    pdf"]
11 },
12 {
13   "value": "Elise Backdoor",
14   "synonyms": ["Elise"]
15 }
```

Groups

Axiom

Beijing Group

Berserk Bear

Boulder Bear

BuhTrap

Event ID	Info	Date	Tags
2499	Operation Buhtrap malware distributed via ammy.com	2015-11-12	Type:OSINT, tlp:white

Charming Kitten

Cleaver

Codoso

Event ID	Info	Date	Tags
3312	OSINT: Exploring Bergard: Old Malware with New Tricks	2016-01-28	circl:incident-classification="malware", osint:source-type="blog-post"
3030	OSINT Codoso APT Yara rules from Loki Scanner by Florian Roth	2016-01-30	Type:OSINT, tlp:white
3016	OSINT - Exploring Bergard: Old Malware with New Tricks	2016-01-28	Type:OSINT, tlp:white
901	OSINT Chinese Espionage Campaign Compromises Forbes.com to Target US Defense, Financial Services Companies in Watering Hole Style Attack by Invincea	2015-02-10	tlp:green, Type:OSINT

Comment Crew

Cutting Kitten

Dagger Panda

Deadeye Jackal

Dizzy Panda

PE indicators

- Original filename
- Compilation timestamp
- Import hashes
- Number of sections
- Entry points
- Soon: API calls
- Soon: Entropy of the sections
- Soon: Fuzzy hashing on the import table

PE indicators

Samples

SHA256	entrypoint	ep_section	timestamp	nb_tls	is_pefile	originalfilename	imphash	timestamp_iso	secnumber	packed
0bc084fa55a03d575e47072004d5532e02c4f6c402d9a02e6ed3190c36a	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
5d42def31722ae8adb350b2982d91fb05a8568876b73b061df3cd0639911b69	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
ed203079a9bd5300dc71644d5c0df609d71d5c1e0d9e39e44ecd81d6237d00	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
aldae5e29a6fcb98a265c2917a81e9ef385e76d2542e0c30c8990bc3311596	9948	.text 0	1340713221	0	True	None	fb84c384095c4cae125e8501a00a114	2012-06-26T14:20:21	6	0
2ed5c6852aeebc73d7f20c188fa4744217d3d388275e115df680c1383a5a814	587912	.text 1	1339153947	0	True	MSRSAAP.EXE	8033c118a21d3c317e8655120579933	2012-06-08T13:12:27	9	0
748d0d0eb2117a36553be4c457b53e9d9845e2543644cd71189351a1efdf8	None	None	None	None	None	None	None	None	None	None
44ebcacc8a04c2ea0d15c204351adee71c3b68a1d99287942ca712341de42a	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
156b1248c0ec8425db8a2895105fec380a4ce03241571c8eb8daaf9a168f	653744	INIT 1	1360325607	0	True	Ultra3.sys	b33e353364d7f5474068496bac228735	2013-02-08T13:13:27	5	90
3746fe217e75ecd84ae124f3b3b18cd4fd37945995134d289591983a2e59299	7286	.text 0	1402804315	0	True	Slm.exe	4f4d33cfdcbadaca4f25d7c6d82ec1830	2014-06-15T05:51:55	4	0
955661448c0c537ab99936da7a853b6b12df0d9f5228acf5887e794abebe	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
a262d9e5855447ebcd3052b06d714c761c0656a5b426944e3b27b4a8a2eb2a7c	18563	.text 0	1361334819	0	True	None	10667bae2ab4615fa97a6d1160a88e87	2013-02-20T05:33:39	4	50
1e705f2ce140118c3b511651604b5e4c37de376442c08213ce20e3081d547a35	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
a5c066639dc9f82b6c7576e4f58442990d16a674304ef9d03cc3a819a1b41f	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
214578079fd01c3c67ca0a16d59d02111a5dfb613bca5120463bda2a6f8dc52	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	0
2d1c036a2cfe11421850ebe46c1177b99087a724760bab8ac217a2c5832d4	587912	.text 1	1339084793	0	True	MSRSAAP.EXE	e5b4359a3773764a372173074ae9b6bd	2012-06-07T11:59:53	9	50
63cc71c2694c74a9f6b6fd333e42d001c8df56641e32af5ab90429853d3d3b	None	None	None	None	None	None	None	None	None	None
a9b308928eb9cdca5136ee37053fa0453a33d0706dcb2343c91013193de761e	13866	.text 0	1347598075	0	True	None	29c56e896bb10003d63af3a464d55e96	2012-09-14T06:47:55	4	0
ee0cb75ea447c03e0445251104458c7c6c8080a7a2603e2e076d1a9455c2325	None	None	None	None	None	None	None	None	None	None
40a7bc2f9ba20af6d9a5c010a6801990de27dd55267297475973293c7091da982	4096	.text 0	1105885028	0	True	None	2c6263c35b5b7685ae76a0bc228b266	2005-01-16T15:17:08	4	0
3eca42780630a0fd8b7e109c8b0e7809f582f96e5284db25995c897e92be	12847	.text 0	1353051322	0	True	None	63M00403dae8328f132b19e7e9b46	2012-11-16T08:35:23	0	0
e898ce6e1391cd09e20c295712db1457d26275816bc8d1e568984b2bee1f	0	[0	1339153947	0	True	MSRSAAP.EXE	68fbcdbac82d6f718e9a2057e56993b	2012-06-08T13:12:27	10	140
c423ee433b77119e198d5ee5b0415e5c476e6b0971617884b847f0d0949	None	None	None	None	None	None	None	None	None	None
065e2217272916093c34ab21722058121a53256e4812b14d909365c325ab9	717232	UPX 1	1261071740	0	True	None	77b2e5e9b22bef763864ab650c59c	2009-12-17T18:42:20	3	140

PE indicators - Compilation Timestamp

Compilation timestamps

Show entries

Search:

Timestamp	Timestamp ISO	Frequency	Unique EventIDs
708992537	1992-06-20T00:22:17	267	25
0	1970-01-01T01:00:00	239	13
1339247989	2012-06-09T15:19:49	64	12
1389106221	2014-01-07T15:50:21	7	7
1400832469	2014-05-23T10:07:49	1	7
1260053452	2009-12-05T23:50:52	30	6
1352800391	2012-11-13T10:53:11	76	6
1374825217	2013-07-26T09:53:37	15	6
1387503293	2013-12-20T02:34:53	3	6
1424692212	2015-02-23T12:50:12	1	6
1048575930	2003-03-25T08:05:30	7	5
1208111565	2008-04-13T20:32:45	9	5
1213313968	2008-06-13T01:39:28	1	5

PE indicators - Compilation Timestamp

Compilation timestamps

1260053452

Merge events

Un-Check All

Event ID	Info	Date	Tags
<input type="checkbox"/> 3801	FBI FLASH A-000071-MW	2016-05-06	MALWARE, tlp:green, APT
<input type="checkbox"/> 2848	OSINT: Novetta WINNTI ANALYSIS	2015-04-06	
<input type="checkbox"/> 2099	TVSPY - Threat Actor Group Reappears with Teamviewer Malware Package	2015-09-03	Type:OSINT, tlp:white
<input type="checkbox"/> 1891	OSINT New Hacking Team IOC's Released by Rook security	2015-07-21	Type:OSINT, tlp:white
<input type="checkbox"/> 1674	OSINT Milano Hacking Team malware detection tool & IOCs by Rook Security	2015-07-21	Type:OSINT, tlp:white
<input type="checkbox"/> 1115	OSINT Winnti OpSMN new malware RE report by Novetta	2015-04-07	Type:OSINT, tlp:white

Sha256

[6e678dc4d933b1865571671913fb2fada37f342d5007dac0b745ca718d2e7405](#)

[72ec760b698dc19693eaa846b2cc21ebccec4ee122feb30cb0802a9920af9898](#)

[7927f3a35d87250253d8abc021d44cc496d2185f376f0d33b0365a68ba81e636](#)

[1b72081c4422785d8c6c016b10bdd7545e5fc611f73277b0366e9b40e624616](#)

[ce5d792faaca61d7bb63367f8772f492ee963f054bc03e61b4fae774c3a3c343](#)

[55c47683e8f7100e4d7175b0eb54ae0f1eab64829b00c9ed4aeafb767fa5d9c5](#)

[d5b3cc429c8a6fba074d9b1e2963273ac13cead47f63dbbb97e640b74e407134](#)

[3087f00b5ef2941ebf3005e9ed46c134a601c629d8dd26e83b25b3e3a4106f77](#)

[257642ee204133025eeead3dc24d9c703f87b77d32ee51eac4f691890e1a593b](#)

[91b0995ee522a6a01fe112dd6cdc21f2cd57b26ac84d8e3065f124ccb93c5eb4](#)

PE indicators - Original Filenames

Original Filenames

Show entries

Search:

Original Filename	Frequency	Unique EventIDs
FlashUtil.exe	21	12
Juniper SSL VPN ActiveX.exe	1	7
msiexec.exe	34	7
WinWord.exe	24	7
chrome.exe	10	6
SecureInput.exe	3	6
svchost.exe	13	6
WEXTRACT.EXE	15	6
WLMerger.exe	71	6
amdocl_as32.exe	2	5
atiapfx.exe	3	5
atiodcli.exe	1	5
atiode.exe	2	5
CONHOST.EXE	3	5
firefox.exe	20	5
FlashPlayerCPLApp.cpl	2	5

PE indicators - Original Filenames

Original Filenames

chrome.exe

Merge events

Un-Check All

Event ID	Info	Date	Tags
<input type="checkbox"/> 3438	The Dukes: 7 Years of Russian Espionage	2015-09-17	tlp:white
<input type="checkbox"/> 2861	OSINT: COSMICDUKE Cosmu with a twist of MiniDuke	2015-12-22	
<input type="checkbox"/> 2465	OSINT Systematic cyber attacks against Israeli and Palestinian targets going on for a year by Norman	2012-10-03	Type:OSINT, tlp:white
<input type="checkbox"/> 2202	OSINT - THE DUKES 7 years of Russian cyberespionage	2015-09-17	Type:OSINT, tlp:white, circ:osint-feed
<input type="checkbox"/> 465	OSINT - MiniDuke 2 (CosmicDuke)	2014-07-02	tlp:green
<input type="checkbox"/> 455	OSINT - COSMICDUKE Cosmu with a twist of MiniDuke	2014-07-02	tlp:green, Type:OSINT

Sha256

[11579b7905eafbd4ae7709bfa880a2442ad37257ebccedd1c6675b6ac45bb0a](#)
[136294c199993886576892d812cd8aab4283fb3de1c2b5de173e404490e4faba](#)
[551af522d2adbc24c3821a3408d231045da0d4dc55ff559b0c9049d36d10a16d](#)
[1fe180e5a40ed462a65444e428b996043decdf863980501c51cbd7e3bd96c6](#)
[70fd11726810e30e4dc34a530edf2b349f913b1e492c73eb1115204fcd3cd59](#)
[c4c477bed7e69b8efac3f6904f8c06889680c590ec728ae59c0ff6e8fa05](#)
[7e371cd323898e403df7a80add34d791e160e443bcd2d02f2ddc0c04ba1bdab](#)
[ca5094b2dbd7a0cc4531034955d4563c0504e1b4ea262ce6b6ff023fbfc06f1c](#)
[9ce93f04dbb6a3b833f1146a54dadfd224fd24e3cca1f8a1eb4e902d597f6](#)
[c759d829478aa8227ad9d27ace855ca5c61ddb9684f321e43e856236dd5bfb61](#)

SSDeep Clustering

- Compute SSDeep hashes on big datasets
- Group samples by similarity
- Allow to pick groups with a certain level of similarities
- Especially interesting on targeted and/or unpacked samples

SSDeep

Group name

ssdeep:group_2794

Merge events

Un-Check All

Event

ID	Info	Date	Tags
<input type="checkbox"/> 3801	FBI FLASH A-000071-MW	2016-05-06	MALWARE, tlp:green, APT
<input type="checkbox"/> 3426	BlackVine - Symantec	2015-07-01	tlp:white
<input type="checkbox"/> 2329	OSINT - I am HDRoot! Part 2	2015-10-13	Type:OSINT, tlp:white
<input type="checkbox"/> 1739	OSINT Technical Analysis Tracks the Sakula Malware Family by SecureWorks	2015-07-30	Type:OSINT, tlp:white, circl:osint-feed
<input type="checkbox"/> 1658	OSINT Black Vine: Formidable cyberespionage group targeted aerospace, healthcare since 2012 by Symantec	2015-07-28	Type:OSINT, tlp:white, circl:osint-feed
<input type="checkbox"/> 623	OSINT - Operation SMN (Novetta)	2014-10-28	TODO:VT-ENRICHMENT, tlp:green, Type:OSINT

Sha256

[23bb555d3039ac59c5c827aefd46b70acdf7ebd284dd8fa2e05282774478f94d](#)

[4086ae5b9737802b6a93a0466d2daf310ba80af82f52b55148b7382b83167bb5](#)

[f0cf68fa2301851b8f65a872b56d735617383349cc73b7eb19ee8ee41fe89b71](#)

MISP Hashstore

- Allow very **fast lookups** against big dataset.
- Only store hashed versions of the attributes.
- Can be used on untrusted or compromised systems (comparable to **bloom filter**).
- Hashstore can be used for forensic analysis (e.g. compare baseline
- Beta version available¹.

¹<https://github.com/MISP/misp-workbench/tree/master/hashstore>

MISP Workbench

- Objective: bundle all the functionalities in one single tool
- Easily **enrich MISP dataset** with other fields (specially PE indicators)
- Simple connectors with other tools and datasets
- **Group events** using galaxies (adversaries and tools)
- **Full text indexing** and lookups for other keywords
- Display the amount of unique MISP events matching a PE attribute
- Single user **lightweight interface**
- Stantalone and offline

Implementation

- Full python 3
- Redis backend
- Whoosh full text indexer
- Pefile for the PE processing, radare2 will be used soon
- Flask + bootstrap web interface

Setup

- Export MySQL to Redis
 - Full snapshot for workbench
 - Partial snapshot for hashstore
- Doesn't respect MISP ACL
- Redis database can be moved to an other system
- Run full text indexing
- Import the PE indicators
- Run ssdeep correlation

Q&A



- Developed in collaboration with Marion Marschalek
- <https://github.com/MISP/misp-workbench>
- <https://github.com/MISP/misp-galaxy>
- <https://github.com/MISP/data-processing>
- <https://github.com/CIRCL/ssdc>
- We welcome new functionalities and pull requests.