TLP:GREEN

Malware hunting with Yara

in mwdb.cert.pl

Jarosław Jedynak

11th CSIRTs Network Meeting
2020-06-04

Agenda

- **Who** am I
- **What** is mwdb
  - **Why** is mwdb
- **What** is mquery
  - **Why** is mquery
- **How** to use them together

$ **who**ami

- Jarosław Jedynak
- Analysis of Current Threats Team @ **CERT.PL**
- **Malware analyst** and software developer

- Long time mwdb user, and backend developer
- Main developer and maintainer of mquery

Agenda

- ✔ ~~**Who** am I~~
- **What** is mwdb
    - **Why** is mwdb
- **What** is mquery
    - **Why** is mquery
- **How** to use them
    - Real-world case studies

What

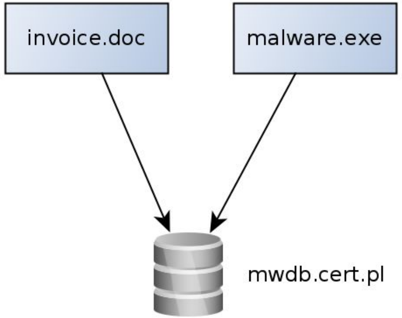
What is mwdb

- **M**al**w**are **d**ata**b**ase

mwdb.cert.pl

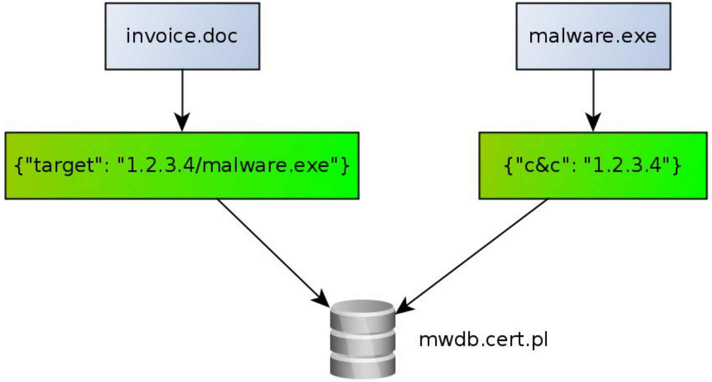
What is mwdb

- **M**al**w**are **d**ata**b**ase
- Repository for files analysed by us



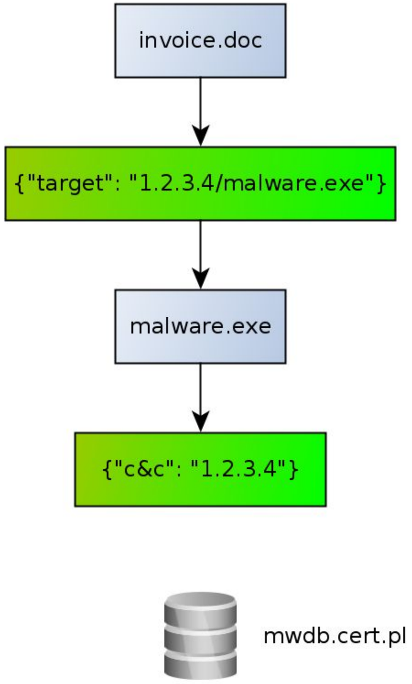
What is mwdb

- **M**al**w**are **d**ata**b**ase
- Repository for files analysed by us
- With extracted configs



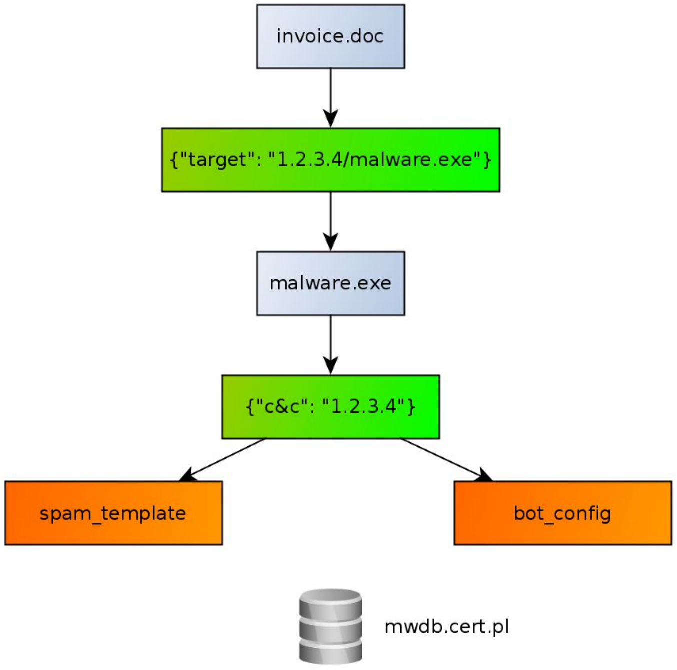
What is mwdb

- **Malware database**
- Repository for files analysed by us
- With extracted configs
- With parent-child relations



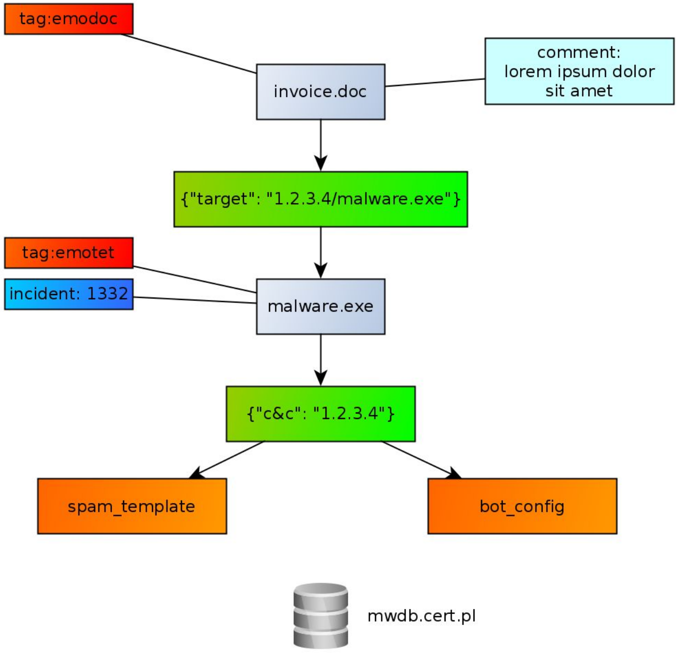
What is mwdb

- **M**alware **d**ata**b**ase
- Repository for files analysed by us
- With extracted configs
- With parent-child relations
- With additional unstructured data



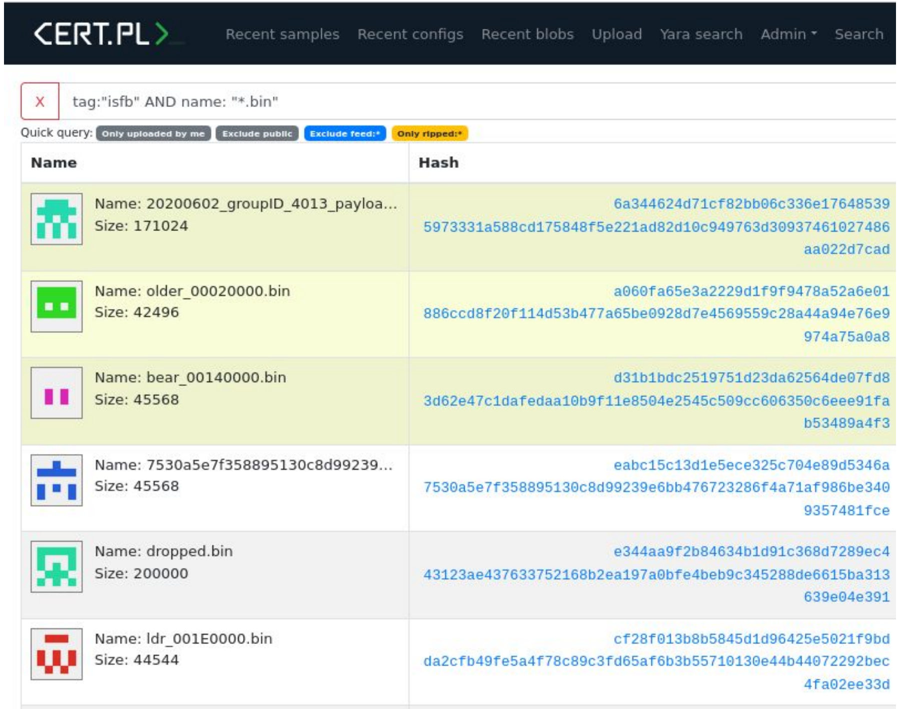
What is mwdb

- **M**alware **d**ata**b**ase
- Repository for files analysed by us
- With extracted configs
- With parent-child relations
- With additional unstructured data
- With tags, comments and metadata



What is mwdb

- **Malware database**
- Repository for files analysed by us
- With extracted configs
- With parent-child relations
- With additional unstructured data
- With tags, comments and metadata
- Queryable (Lucene syntax)

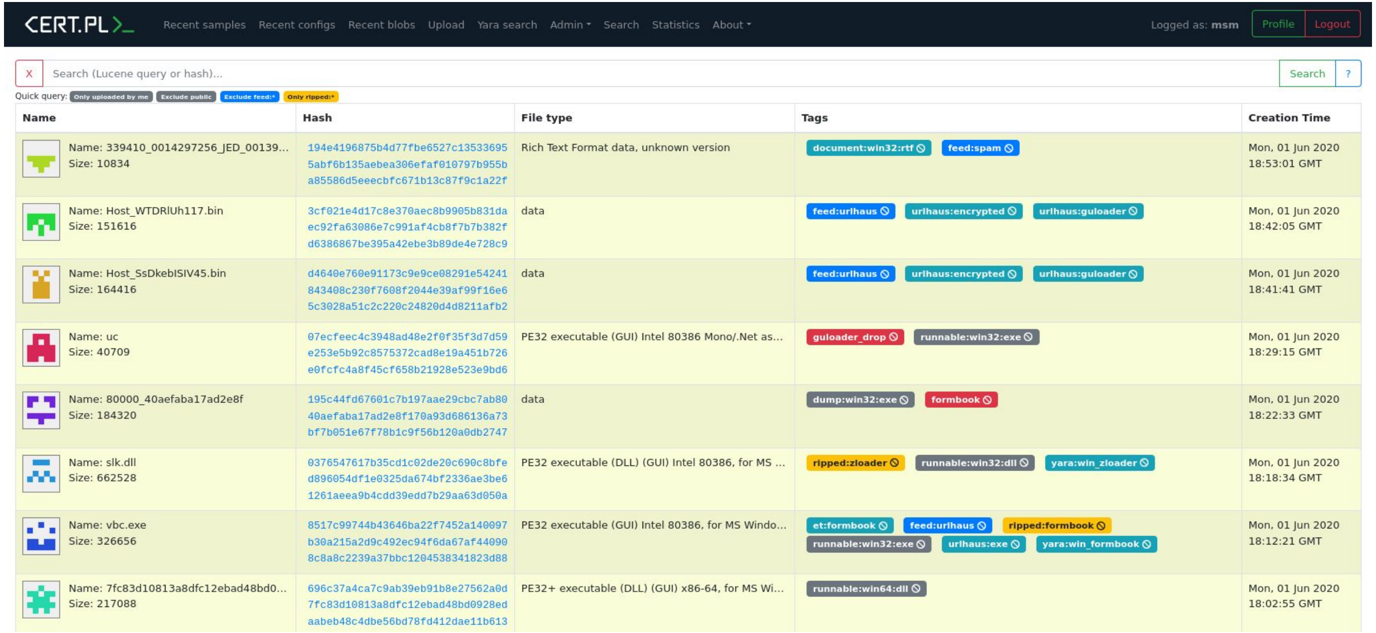


tag:"isfb" AND name: "*.bin"

Quick query: Only uploaded by me | Exclude public | Exclude feed:* | Only ripped:*

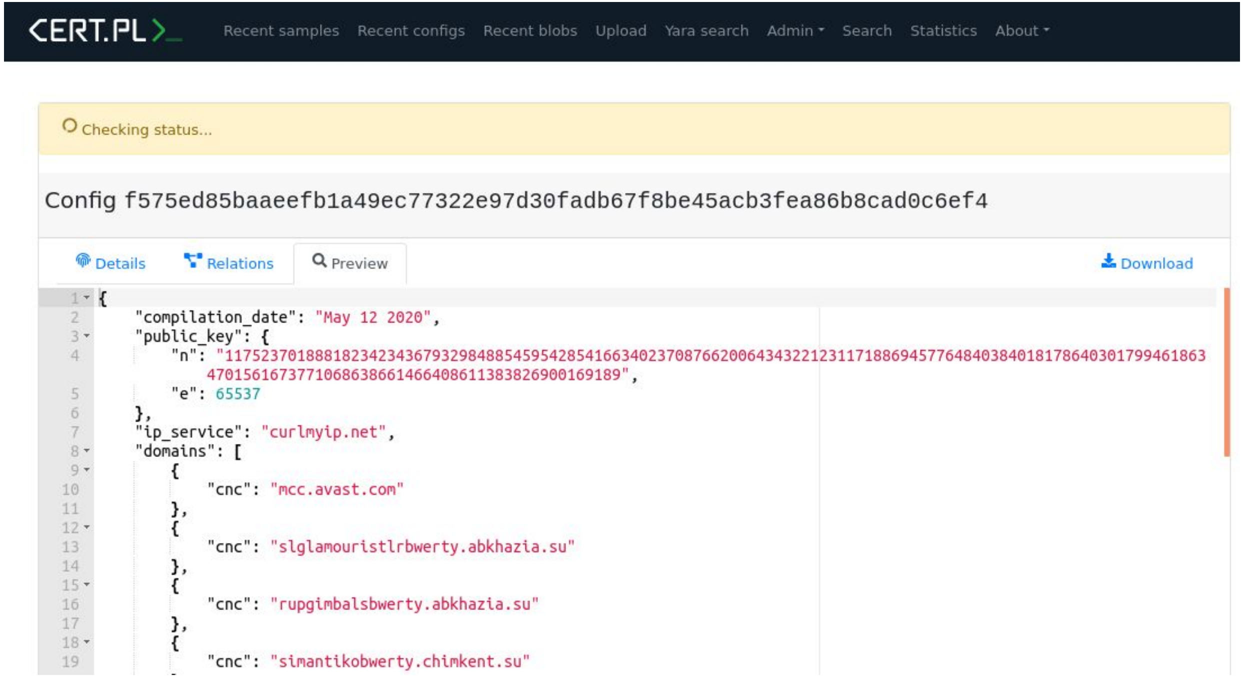
Name	Hash
Name: 20200602_groupID_4013_payloa... Size: 171024	6a344624d71cf82bb06c336e176485395973331a588cd175848f5e221ad82d10c949763d30937461027486aa022d7cad
Name: older_00020000.bin Size: 42496	a060fa65e3a2229d1f9f9478a52a6e01886ccd8f20f114d53b477a65be0928d7e4569559c28a44a94e76e9974a75a0a8
Name: bear_00140000.bin Size: 45568	d31b1bdc2519751d23da62564de07fd83d62e47c1dafedaa10b9f11e8504e2545c509cc606350c6eee91fab53489a4f3
Name: 7530a5e7f358895130c8d99239... Size: 45568	eabc15c13d1e5ece325c704e89d5346a7530a5e7f358895130c8d99239e6bb476723286f4a71af986be3409357481fce
Name: dropped.bin Size: 200000	e344aa9f2b84634b1d91c368d7289ec443123ae437633752168b2ea197a0bfe4beb9c345288de6615ba313639e04e391
Name: ldr_001E0000.bin Size: 44544	cf28f013b8b5845d1d96425e5021f9bdda2cfb49fe5a4f78c89c3fd65af6b3b55710130e44b44072292bec4fa02ee33d

What is mwdb



Name	Hash	File type	Tags	Creation Time
Name: 339410_0014297256_JED_00139... Size: 10834	194e4196875b4d77fbe6527c13533695 5abf6b135aebea306efaf010797b955b a85586d5eeecbfc671b13c87f9c1a22f	Rich Text Format data, unknown version	document:win32:rtf feed:spam	Mon, 01 Jun 2020 18:53:01 GMT
Name: Host_WTDRlUh117.bin Size: 151616	3cf021e4d17c8e370aec8b9905b831da ec92fa63086e7c991af4cb8f7b7b382f d6386867be395a42ebe3b89de4e728c9	data	feed:urlhaus urlhaus:encrypted urlhaus:guloader	Mon, 01 Jun 2020 18:42:05 GMT
Name: Host_SsDkebISIV45.bin Size: 164416	d4640e760e91173c9e9ce08291e54241 843408c230f7608f2044e39af99f16e6 5c3028a51c2c220c24820d4d8211afb2	data	feed:urlhaus urlhaus:encrypted urlhaus:guloader	Mon, 01 Jun 2020 18:41:41 GMT
Name: uc Size: 40709	07ecfeec4c3948ad48e2f0f35f3d7d59 e253e5b92c8575372cad8e19a451b726 e0fcfc4a8f45cf658b21928e523e9bd6	PE32 executable (GUI) Intel 80386 Mono/.Net as...	guloader_drop runnable:win32:exe	Mon, 01 Jun 2020 18:29:15 GMT
Name: 80000_40aefaba17ad2e8f Size: 184320	195c44fd67601c7b197aae29cbc7ab80 40aefaba17ad2e8f170a93d686136a73 bf7b051e67f78b1c9f56b120a0db2747	data	dump:win32:exe formbook	Mon, 01 Jun 2020 18:22:33 GMT
Name: slk.dll Size: 662528	0376547617b35cd1c02de20c690c8bfe d896054df1e0325da674bf2336ae3be6 1261aeea9b4cdd39edd7b29aa63d050a	PE32 executable (DLL) (GUI) Intel 80386, for MS ...	ripped:zloader runnable:win32:dll yara:win_zloader	Mon, 01 Jun 2020 18:18:34 GMT
Name: vbc.exe Size: 326656	8517c99744b43646ba22f7452a140097 b30a215a2d9c492ec94f6da67af44090 8c8a8c2239a37bbc1204538341823d88	PE32 executable (GUI) Intel 80386, for MS Windo...	et:formbook feed:urlhaus ripped:formbook runnable:win32:exe urlhaus:exe yara:win_formbook	Mon, 01 Jun 2020 18:12:21 GMT
Name: 7fc83d10813a8dfc12ebad48bd0... Size: 217088	696c37a4ca7c9ab39eb91b8e27562a0d 7fc83d10813a8dfc12ebad48bd0928ed aabeb48c4dbe56bd78fd412dae11b613	PE32+ executable (DLL) (GUI) x86-64, for MS Wi...	runnable:win64:dll	Mon, 01 Jun 2020 18:02:55 GMT

What is mwdb

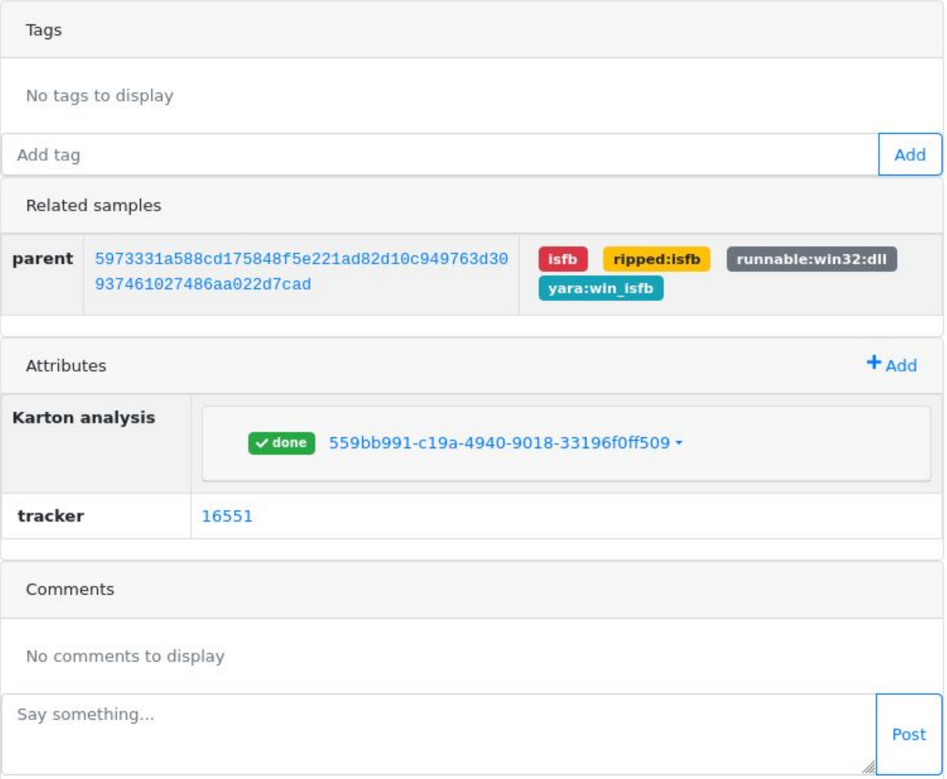


Checking status...

Config f575ed85baaeefb1a49ec77322e97d30fadb67f8be45acb3fea86b8cad0c6ef4

```
{
    "compilation_date": "May 12 2020",
    "public_key": {
        "n": "1175237018881823423436793298488545954285416634023708766200643432212311718869457764840384018178640301799461863
              4701561673771068638661466408611383826900169189",
        "e": 65537
    },
    "ip_service": "curlmyip.net",
    "domains": [
        {
            "cnc": "mcc.avast.com"
        },
        {
            "cnc": "slglamouristlrbwerty.abkhazia.su"
        },
        {
            "cnc": "rupgimbalsbwerty.abkhazia.su"
        },
        {
            "cnc": "simantikobwerty.chimkent.su"
```

What is mwdb



Tags

No tags to display

Related samples

parent	5973331a588cd175848f5e221ad82d10c949763d30937461027486aa022d7cad	isfb ripped:isfb runnable:win32:dll yara:win_isfb

Attributes

Karton analysis	✓ done 559bb991-c19a-4940-9018-33196f0ff509
tracker	16551

Comments

No comments to display

Why not MISP? 🤔

How is it different than MISP? 🤔

How is it different than MISP? 🤔

MISP

- Malware Information Sharing Platform

MWDB

- Malware Database

How is it different than MISP? 🤔

MISP

- ~~Malware~~ General-purpose Information Sharing Platform

MWDB

- Malware Database

How is it different than MISP? 🤔

MISP	MWDB
~~Malware~~ General-purpose Information Sharing Platform	Malware Database
Share indicators with other teams	Frontend for our analytic system

How is it different than MISP? 🤔

MISP

- ~~Malware~~ General-purpose Information Sharing Platform
- Share indicators with other teams

MWDB

- Malware Database
- Frontend for our analytic system (but also a sharing platform ¯_(ツ)_/¯)

How is it different than MISP? 🤔

MISP	MWDB
~~Malware~~ General-purpose Information Sharing Platform	Malware Database
Share indicators with other teams	Frontend for our analytic system (but also a sharing platform ¯_(ツ)_/¯)
Open Source	**Not** Open Source yet

How is it different than MISP? 🤔

MISP	MWDB
~~Malware~~ General-purpose Information Sharing Platform	Malware Database
Share indicators with other teams	Frontend for our analytic system (but also a sharing platform ¯_(ツ)_/¯)
Open Source	**Not** Open Source yet (release of v2 next month!)

How is it different than MISP? 🤔

MISP	**MWDB**
~~Malware~~ General-purpose Information Sharing Platform	Malware Database
Share indicators with other teams	Frontend for our analytic system (but also a sharing platform ¯_(ツ)_/¯)
Open Source	**Not** Open Source yet (release of v2 next month!)
	But you can use our instance!

How is it different than MISP? 🤔

MISP

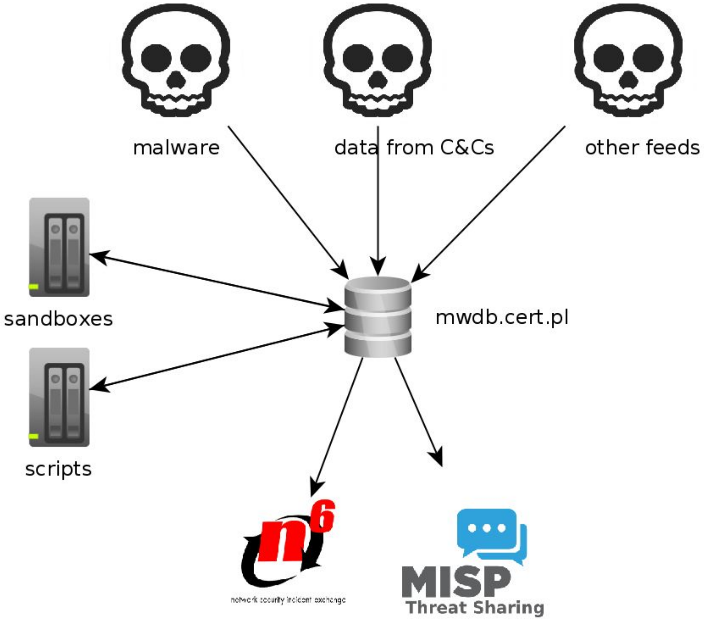
- ~~Malware~~ General-purpose Information Sharing Platform
- Share indi
- Open Source

MWDB

- Malware Database
- nalytic system
  tform ¯_(ツ)_/¯)
- **Not** Open Source yet
  (release of v2 next month!)
- But you can use our instance!

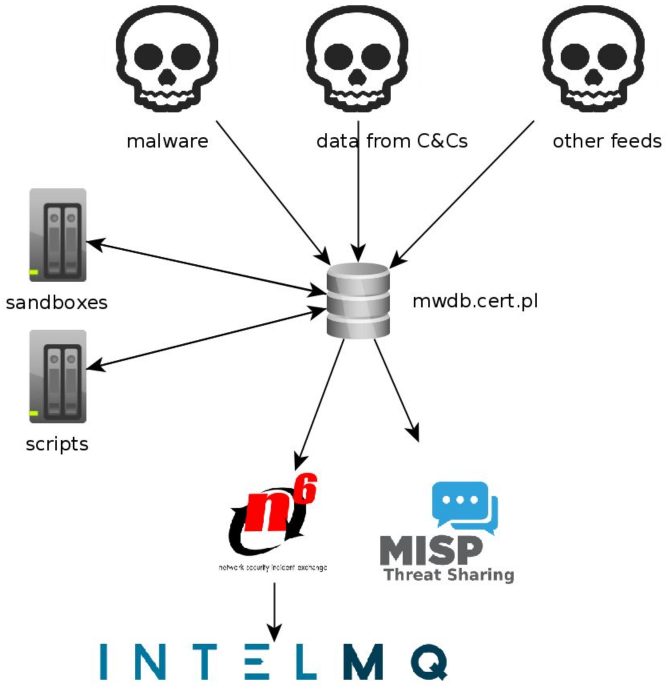
Verdict: Despite all the similarities, not directly competing solutions

How is it different than MISP

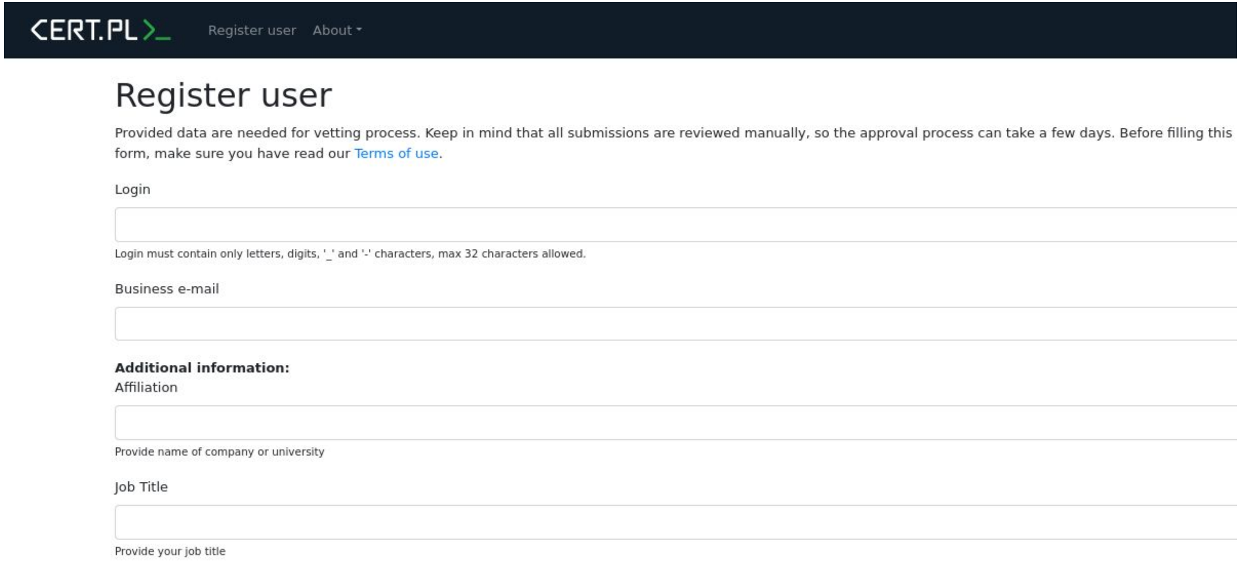


TLP:GREEN

How is it different than MISP



How can I access it?



Register user

Provided data are needed for vetting process. Keep in mind that all submissions are reviewed manually, so the approval process can take a few days. Before filling this form, make sure you have read our Terms of use.

Login

Login must contain only letters, digits, '_' and '-' characters, max 32 characters allowed.

Business e-mail

Additional information:

Affiliation

Provide name of company or university

Job Title

Provide your job title

Access for **all CNW teams**, request an account https://mwdb.cert.pl/register

Agenda

- ✔ ~~**Who** am I~~
- ✔ ~~**What** is mwdb~~
  - ✔ ~~**Why** is mwdb~~
- **What** is mquery
  - **Why** is mquery
- **How** to use them
  - Real-world case studies

What is mquery

~~What~~ **Why** is mquery

- The next logical step after mwdb

~~What~~ **Why** is mquery

- The next logical step after mwdb
- We have a huge collection of samples but no efficient way to query them for content

What is mquery

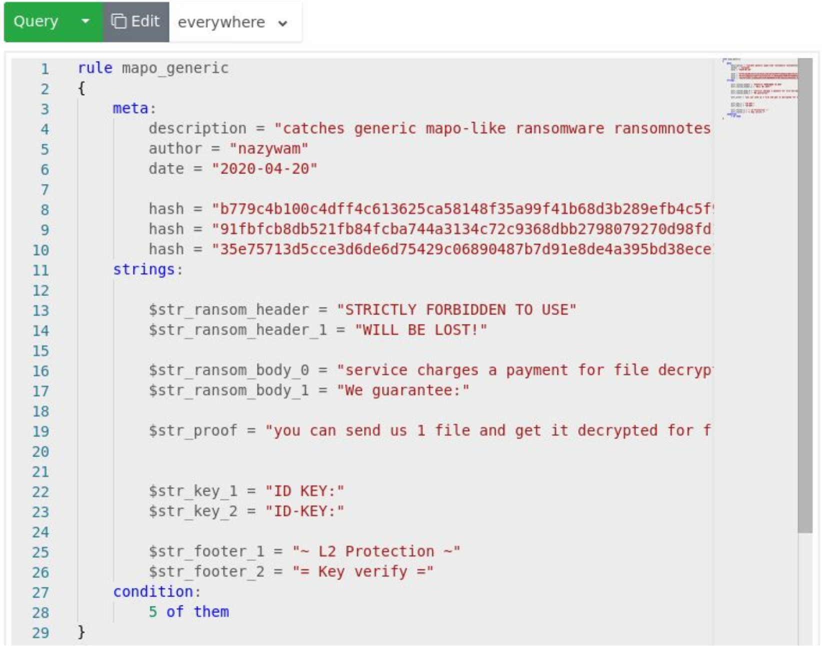
- The next logical step after mwdb
- We have a huge collection of samples but no efficient way to query them for content

mquery

What is mquery

- The next logical step after mwdb
- We have a huge collection of samples but no efficient way to query them for content

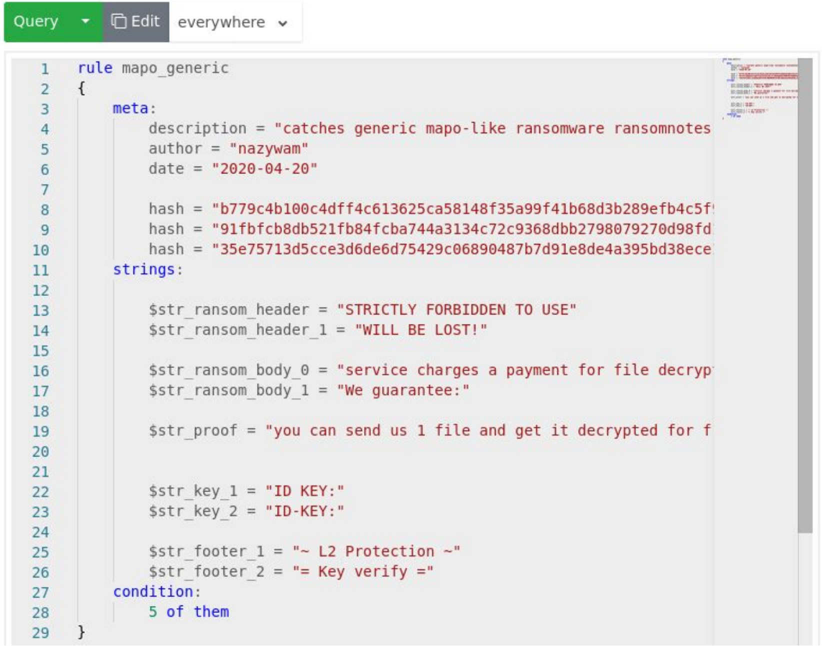
mquery



```
rule mapo_generic
{
    meta:
        description = "catches generic mapo-like ransomware ransomnotes
        author = "nazywam"
        date = "2020-04-20"

        hash = "b779c4b100c4dff4c613625ca58148f35a99f41b68d3b289efb4c5f
        hash = "91fbfcb8db521fb84fcba744a3134c72c9368dbb2798079270d98fd
        hash = "35e75713d5cce3d6de6d75429c06890487b7d91e8de4a395bd38ece
    strings:

        $str_ransom_header = "STRICTLY FORBIDDEN TO USE"
        $str_ransom_header_1 = "WILL BE LOST!"

        $str_ransom_body_0 = "service charges a payment for file decryp
        $str_ransom_body_1 = "We guarantee:"

        $str_proof = "you can send us 1 file and get it decrypted for f


        $str_key_1 = "ID KEY:"
        $str_key_2 = "ID-KEY:"

        $str_footer_1 = "~ L2 Protection ~"
        $str_footer_2 = "= Key verify ="
    condition:
        5 of them
}
```

What is mquery

- The next logical step after mwdb
- We have a huge collection of samples but no efficient way to query them for content



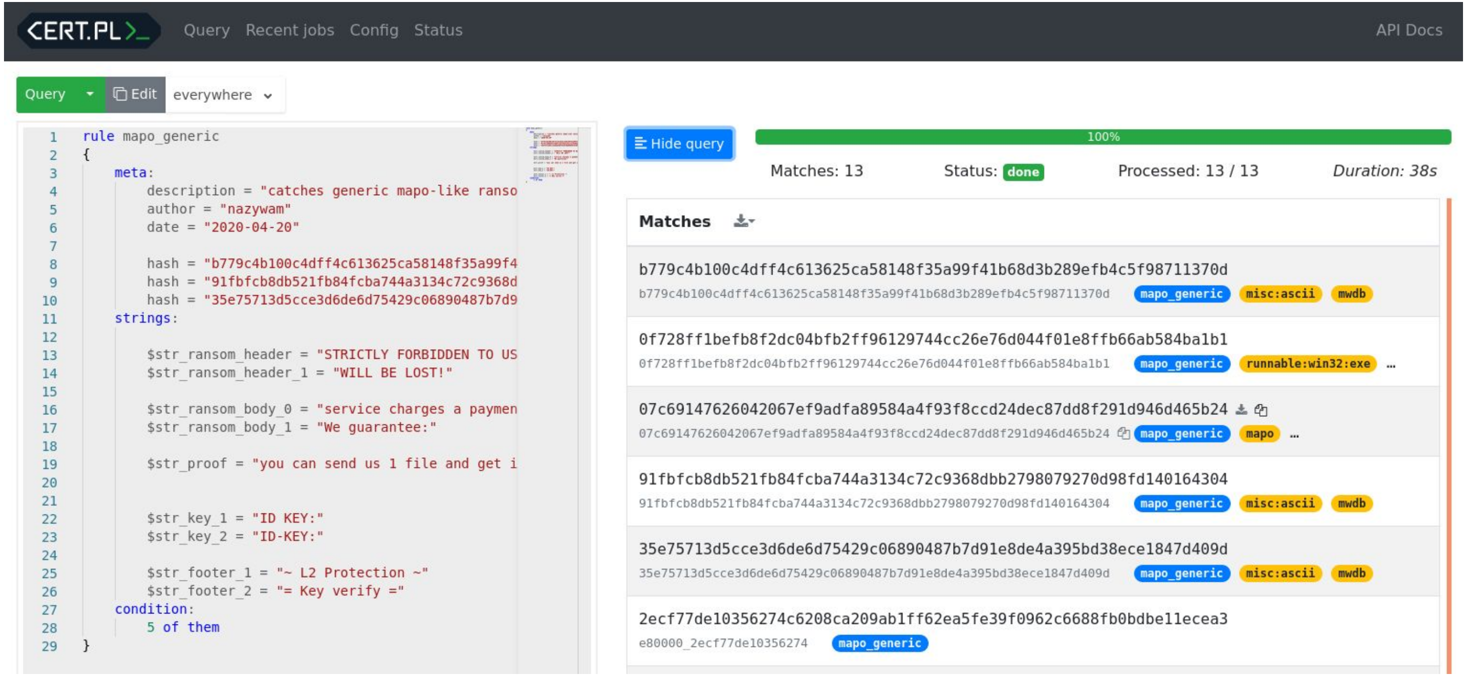
```
rule mapo_generic
{
    meta:
        description = "catches generic mapo-like ransomware ransomnotes
        author = "nazywam"
        date = "2020-04-20"

        hash = "b779c4b100c4dff4c613625ca58148f35a99f41b68d3b289efb4c5f
        hash = "91fbfcb8db521fb84fcba744a3134c72c9368dbb2798079270d98fd
        hash = "35e75713d5cce3d6de6d75429c06890487b7d91e8de4a395bd38ece
    strings:

        $str_ransom_header = "STRICTLY FORBIDDEN TO USE"
        $str_ransom_header_1 = "WILL BE LOST!"

        $str_ransom_body_0 = "service charges a payment for file decryp
        $str_ransom_body_1 = "We guarantee:"

        $str_proof = "you can send us 1 file and get it decrypted for f


        $str_key_1 = "ID KEY:"
        $str_key_2 = "ID-KEY:"

        $str_footer_1 = "~ L2 Protection ~"
        $str_footer_2 = "= Key verify ="
    condition:
        5 of them
}
```

mquery

For so-called malware hunting

TLP:GREEN

What is mquery



```
rule mapo_generic
{
    meta:
        description = "catches generic mapo-like ranso
        author = "nazywam"
        date = "2020-04-20"

        hash = "b779c4b100c4dff4c613625ca58148f35a99f4
        hash = "91fbfcb8db521fb84fcba744a3134c72c9368d
        hash = "35e75713d5cce3d6de6d75429c06890487b7d9
    strings:

        $str_ransom_header = "STRICTLY FORBIDDEN TO US
        $str_ransom_header_1 = "WILL BE LOST!"

        $str_ransom_body_0 = "service charges a paymen
        $str_ransom_body_1 = "We guarantee:"

        $str_proof = "you can send us 1 file and get i


        $str_key_1 = "ID KEY:"
        $str_key_2 = "ID-KEY:"

        $str_footer_1 = "~ L2 Protection ~"
        $str_footer_2 = "= Key verify ="
    condition:
        5 of them
}
```

Matches: 13 Status: done Processed: 13 / 13 *Duration: 38s*

Matches

b779c4b100c4dff4c613625ca58148f35a99f41b68d3b289efb4c5f98711370d
b779c4b100c4dff4c613625ca58148f35a99f41b68d3b289efb4c5f98711370d mapo_generic misc:ascii mwdb

0f728ff1befb8f2dc04bfb2ff96129744cc26e76d044f01e8ffb66ab584ba1b1
0f728ff1befb8f2dc04bfb2ff96129744cc26e76d044f01e8ffb66ab584ba1b1 mapo_generic runnable:win32:exe ...

07c69147626042067ef9adfa89584a4f93f8ccd24dec87dd8f291d946d465b24
07c69147626042067ef9adfa89584a4f93f8ccd24dec87dd8f291d946d465b24 mapo_generic mapo ...

91fbfcb8db521fb84fcba744a3134c72c9368dbb2798079270d98fd140164304
91fbfcb8db521fb84fcba744a3134c72c9368dbb2798079270d98fd140164304 mapo_generic misc:ascii mwdb

35e75713d5cce3d6de6d75429c06890487b7d91e8de4a395bd38ece1847d409d
35e75713d5cce3d6de6d75429c06890487b7d91e8de4a395bd38ece1847d409d mapo_generic misc:ascii mwdb

2ecf77de10356274c6208ca209ab1ff62ea5fe39f0962c6688fb0bdbe11ecea3
e80000_2ecf77de10356274 mapo_generic

Agenda

- ✔ ~~Who am I~~
- ~~✔ What is mwdb~~
  - ~~✔ Why is mwdb~~
- ~~✔ What is mquery~~
  - ~~✔ Why is mquery~~
- **How** to use them
  - Real-world case studies

How can I access it?

How can I access it?

	Community access?	
mwdb	✔	
mquery	✘	

How can I access it?

	Community access?	Open source?
mwdb	✔	WIP
mquery	✘	✔

TLP:GREEN

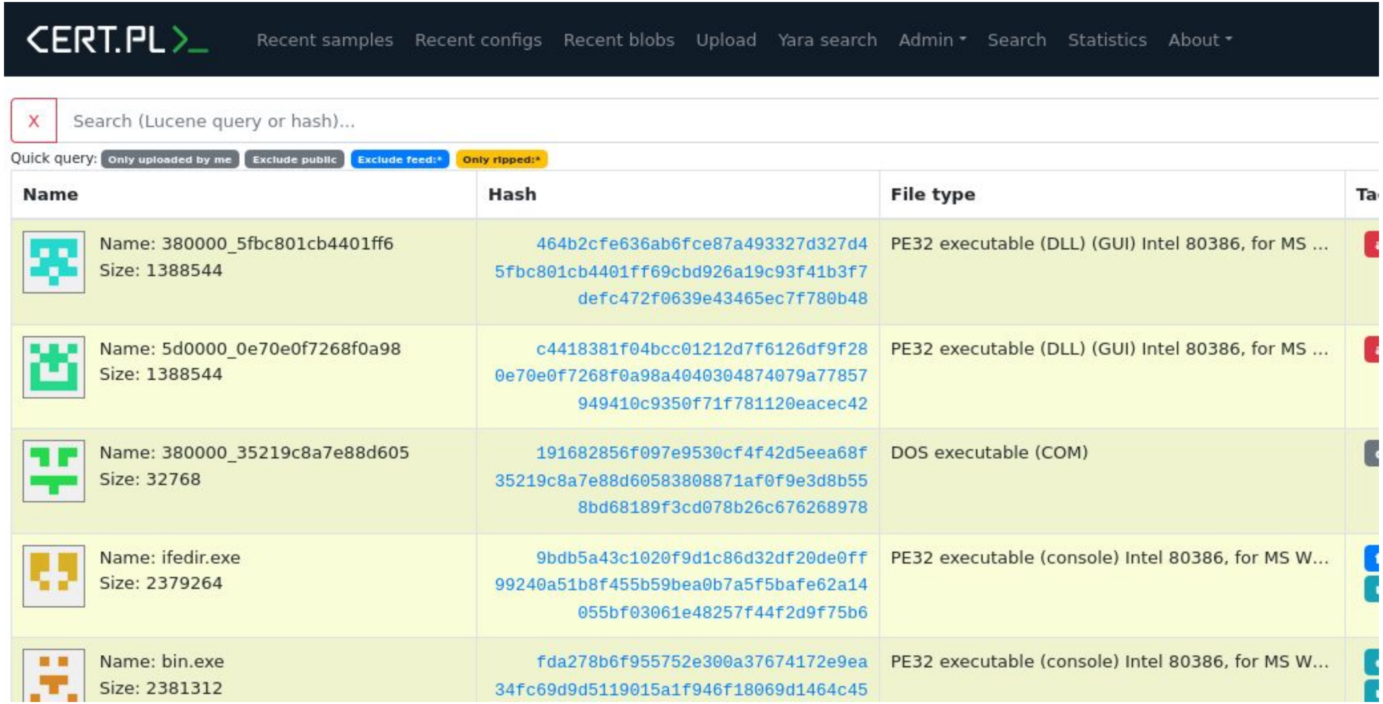
How can I access it?

	Community access?	Open source?
mwdb	✔	**WIP**
mquery	**WIP?**	✔

How can I access it?

	Community access?	Open source?
mwdb	✔	**WIP**
mquery	**WIP?**	✔
mquery via mwdb	✔	**WIP**

mquery + mwdb

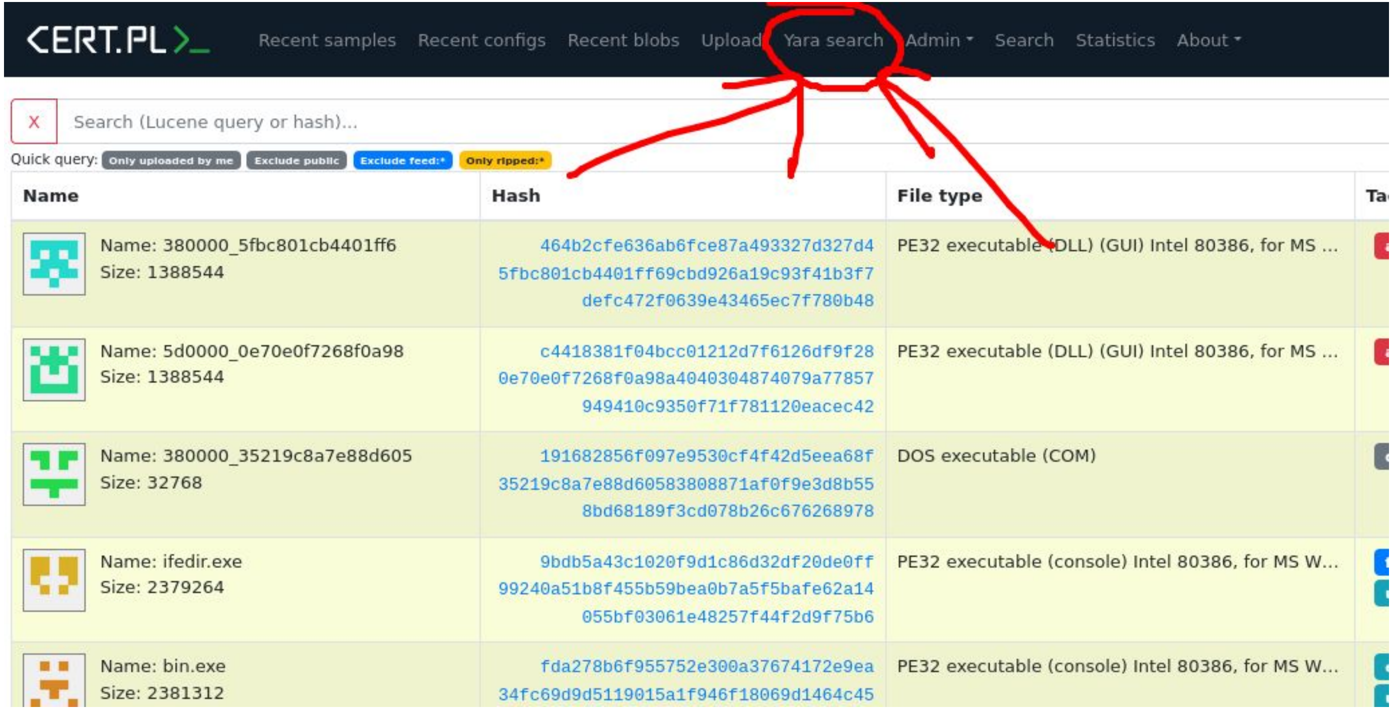


Quick query: Only uploaded by me Exclude public Exclude feed:* Only ripped:*

Name	Hash	File type	Ta
Name: 380000_5fbc801cb4401ff6 Size: 1388544	464b2cfe636ab6fce87a493327d327d4 5fbc801cb4401ff69cbd926a19c93f41b3f7 defc472f0639e43465ec7f780b48	PE32 executable (DLL) (GUI) Intel 80386, for MS ...	
Name: 5d0000_0e70e0f7268f0a98 Size: 1388544	c4418381f04bcc01212d7f6126df9f28 0e70e0f7268f0a98a4040304874079a77857 949410c9350f71f781120eacec42	PE32 executable (DLL) (GUI) Intel 80386, for MS ...	
Name: 380000_35219c8a7e88d605 Size: 32768	191682856f097e9530cf4f42d5eea68f 35219c8a7e88d60583808871af0f9e3d8b55 8bd68189f3cd078b26c676268978	DOS executable (COM)	
Name: ifedir.exe Size: 2379264	9bdb5a43c1020f9d1c86d32df20de0ff 99240a51b8f455b59bea0b7a5f5bafe62a14 055bf03061e48257f44f2d9f75b6	PE32 executable (console) Intel 80386, for MS W...	
Name: bin.exe Size: 2381312	fda278b6f955752e300a37674172e9ea 34fc69d9d5119015a1f946f18069d1464c45	PE32 executable (console) Intel 80386, for MS W...	

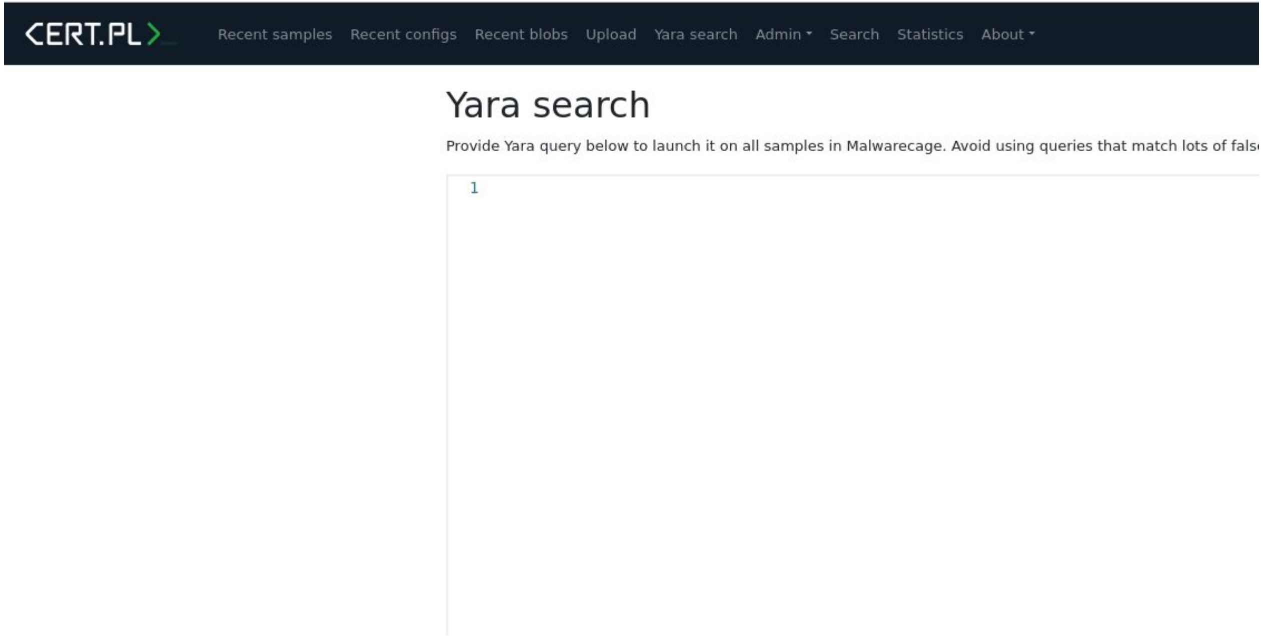
TLP:GREEN

mquery + mwdb



Name	Hash	File type	Ta
Name: 380000_5fbc801cb4401ff6 Size: 1388544	464b2cfe636ab6fce87a493327d327d4 5fbc801cb4401ff69cbd926a19c93f41b3f7 defc472f0639e43465ec7f780b48	PE32 executable (DLL) (GUI) Intel 80386, for MS ...	
Name: 5d0000_0e70e0f7268f0a98 Size: 1388544	c4418381f04bcc01212d7f6126df9f28 0e70e0f7268f0a98a4040304874079a77857 949410c9350f71f781120eacec42	PE32 executable (DLL) (GUI) Intel 80386, for MS ...	
Name: 380000_35219c8a7e88d605 Size: 32768	191682856f097e9530cf4f42d5eea68f 35219c8a7e88d60583808871af0f9e3d8b55 8bd68189f3cd078b26c676268978	DOS executable (COM)	
Name: ifedir.exe Size: 2379264	9bdb5a43c1020f9d1c86d32df20de0ff 99240a51b8f455b59bea0b7a5f5bafe62a14 055bf03061e48257f44f2d9f75b6	PE32 executable (console) Intel 80386, for MS W...	
Name: bin.exe Size: 2381312	fda278b6f955752e300a37674172e9ea 34fc69d9d5119015a1f946f18069d1464c45	PE32 executable (console) Intel 80386, for MS W...	

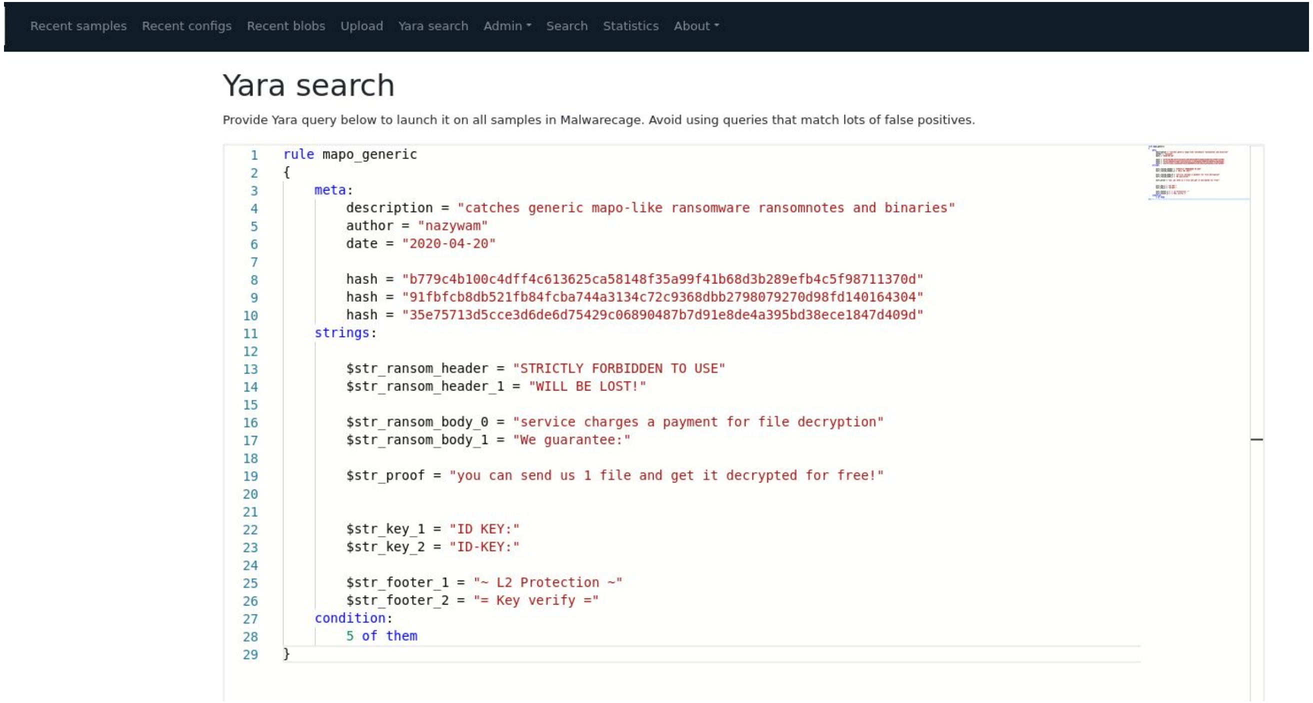
mquery + mwdb



Yara search

Provide Yara query below to launch it on all samples in Malwarecage. Avoid using queries that match lots of fals

mquery + mwdb

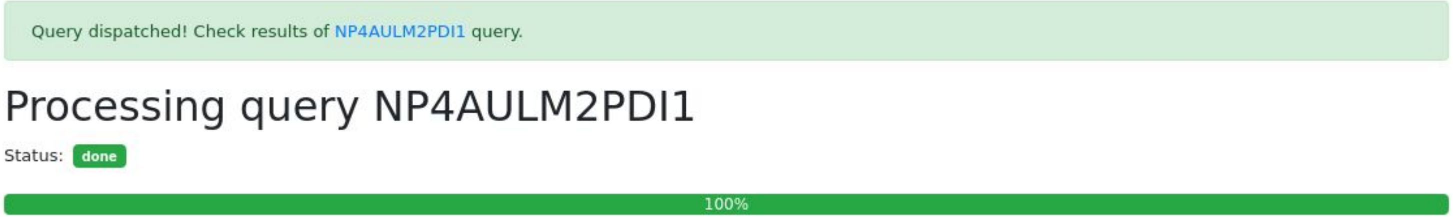


Yara search

Provide Yara query below to launch it on all samples in Malwarecage. Avoid using queries that match lots of false positives.

```
rule mapo_generic
{
    meta:
        description = "catches generic mapo-like ransomware ransomnotes and binaries"
        author = "nazywam"
        date = "2020-04-20"

        hash = "b779c4b100c4dff4c613625ca58148f35a99f41b68d3b289efb4c5f98711370d"
        hash = "91fbfcb8db521fb84fcba744a3134c72c9368dbb2798079270d98fd140164304"
        hash = "35e75713d5cce3d6de6d75429c06890487b7d91e8de4a395bd38ece1847d409d"
    strings:

        $str_ransom_header = "STRICTLY FORBIDDEN TO USE"
        $str_ransom_header_1 = "WILL BE LOST!"

        $str_ransom_body_0 = "service charges a payment for file decryption"
        $str_ransom_body_1 = "We guarantee:"

        $str_proof = "you can send us 1 file and get it decrypted for free!"


        $str_key_1 = "ID KEY:"
        $str_key_2 = "ID-KEY:"

        $str_footer_1 = "~ L2 Protection ~"
        $str_footer_2 = "= Key verify ="
    condition:
        5 of them
}
```

mquery + mwdb



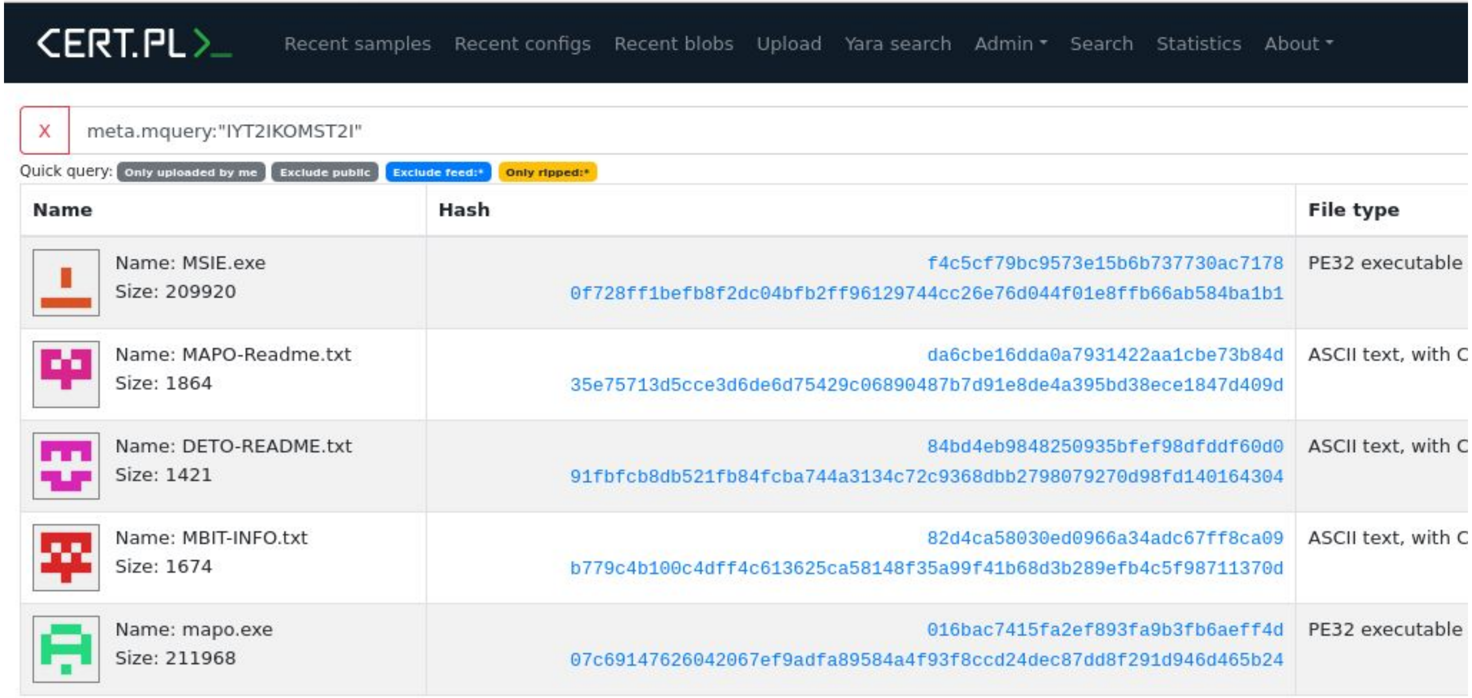
Query dispatched! Check results of NP4AULM2PDI1 query.

Processing query NP4AULM2PDI1

Status: done

100%

mquery + mwdb



meta.mquery:"IYT2IKOMST2I"

Name	Hash	File type
Name: MSIE.exe Size: 209920	f4c5cf79bc9573e15b6b737730ac7178 0f728ff1befb8f2dc04bfb2ff96129744cc26e76d044f01e8ffb66ab584ba1b1	PE32 executable
Name: MAPO-Readme.txt Size: 1864	da6cbe16dda0a7931422aa1cbe73b84d 35e75713d5cce3d6de6d75429c06890487b7d91e8de4a395bd38ece1847d409d	ASCII text, with C
Name: DETO-README.txt Size: 1421	84bd4eb9848250935bfef98dfddf60d0 91fbfcb8db521fb84fcba744a3134c72c9368dbb2798079270d98fd140164304	ASCII text, with C
Name: MBIT-INFO.txt Size: 1674	82d4ca58030ed0966a34adc67ff8ca09 b779c4b100c4dff4c613625ca58148f35a99f41b68d3b289efb4c5f98711370d	ASCII text, with C
Name: mapo.exe Size: 211968	016bac7415fa2ef893fa9b3fb6aeff4d 07c69147626042067ef9adfa89584a4f93f8ccd24dec87dd8f291d946d465b24	PE32 executable

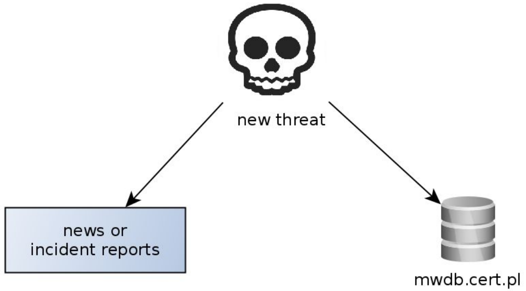
mquery + mwdb

- We made a large part of our malware collection available for researches
- Currently only files uploaded to mwdb can be queried
- In the future, we’ll add even more samples, including large public collections
- There is a slight lag between file upload and indexing (up to 24h)

TLP:GREEN

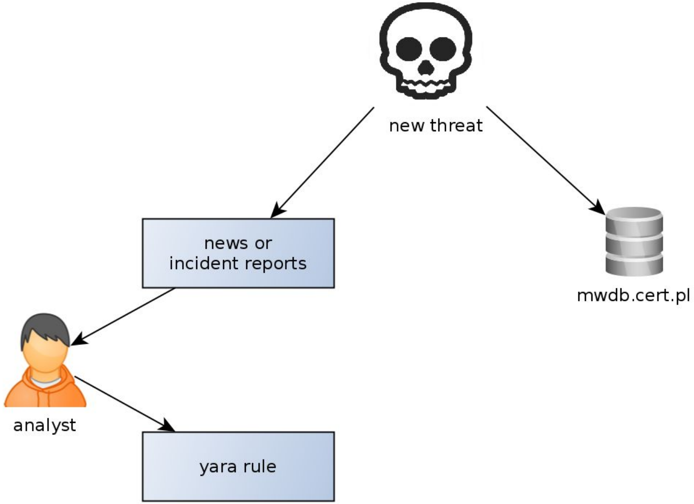
mquery + mwdb

1. New threat identified



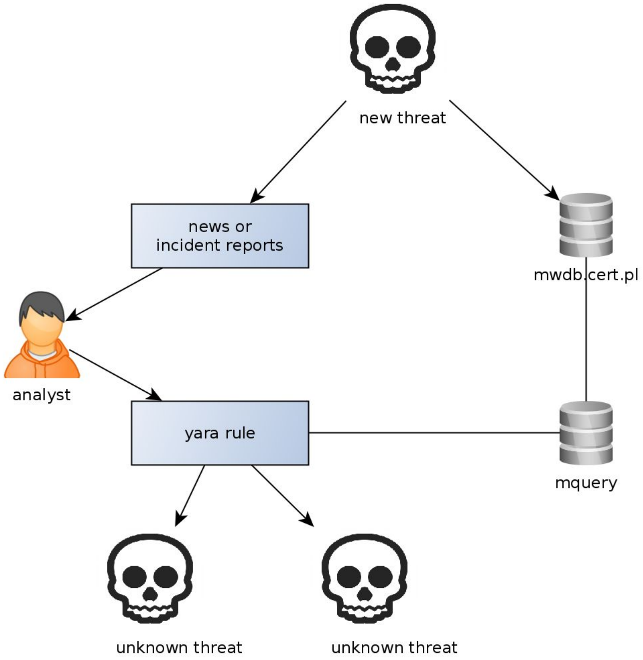
mquery + mwdb

1. New threat identified
2. Threat analysis
   - Create new signatures
   - Update analytic backend



mquery + mwdb

1. New threat identified
2. Threat analysis
   - Create new signatures
   - Update analytic backend
3. Detect and track the campaign



Acknowledgements

Thanks to **Paweł Srokosz**

Main developer, designer and current maintainer of mwdb

Everyone else in CERT.PL

Questions?

Contact:

msm@cert.pl

jaroslaw.jedynak@cert.pl

Co-financed by the Connecting Europe
Facility of the European Union