Wykrywanie złośliwych plików?

Ale co w tym trudnego?

Tytułem wstępu

Reverse Engineering w

Tytułem wstępu

Reverse Engineering w

CERT.PL >_

Kiedyś też

Google

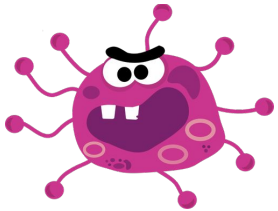
Tytułem wstępu

Reverse Engineering w

CERT.PL >_

Kiedyś też

Symantec Google

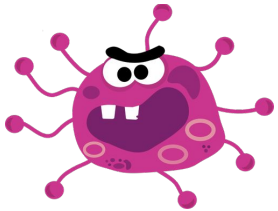


Tytułem wstępu

Reverse Engineering w CERT.PL >_

Kiedyś też Symantec Google

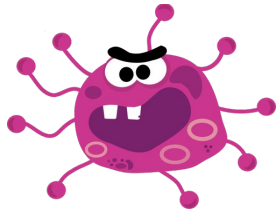
Jaki w ogóle jest problem?



Tytułem wstępu

Reverse Engineering w CERT.PL >_

Kiedyś też Symantec Google



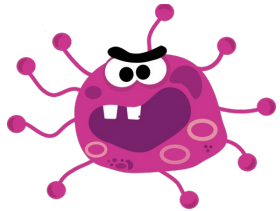
? Jaki w ogóle jest problem?

?? Jak go chcemy rozwiązać?

Tytułem wstępu

Reverse Engineering w CERT.PL >_

Kiedyś też Symantec Google



? Jaki w ogóle jest problem?

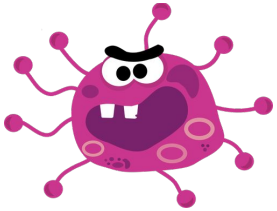
?? Jak go chcemy rozwiązać?

??? Co nam (i wam) to da?

Tytułem wstępu

Reverse Engineering w CERT.PL >_

Kiedyś też Symantec Google



? Jaki w ogóle jest problem?

?? Jak go chcemy rozwiązać?

??? Co nam (i wam) to da?

Ok, tyle wstępu

Część 1

Jaki w ogóle jest problem?

Problem

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

Problem

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym

Poczta Polska S.A.
e-faktura.cof@avitallink.biz

Reply | Forward | Archive | Junk | Delete | More

eFaktura nr: F44556P0825SFAKAMC dla umowy ID: 384665 — 11/12/25, 13:13

Dzień dobry

Poczta Polska S.A. informuje, że dla umowy 384665/G (ID 384665) został wystawiony dokument rozliczeniowy Faktura VAT o numerze: F44556P0825SFAKAMC.

Dziękujemy za terminowe regulowanie płatności.

W przypadku faktur korygujących z kwotą do zwrotu, dla których niezbędne jest uzgodnienie sposobu rozliczenia przedmiot

1. w ramach płatności przez Klienta za fakturę pierwotną kwota zostanie pomniejszona o wartość „do zwrotu”

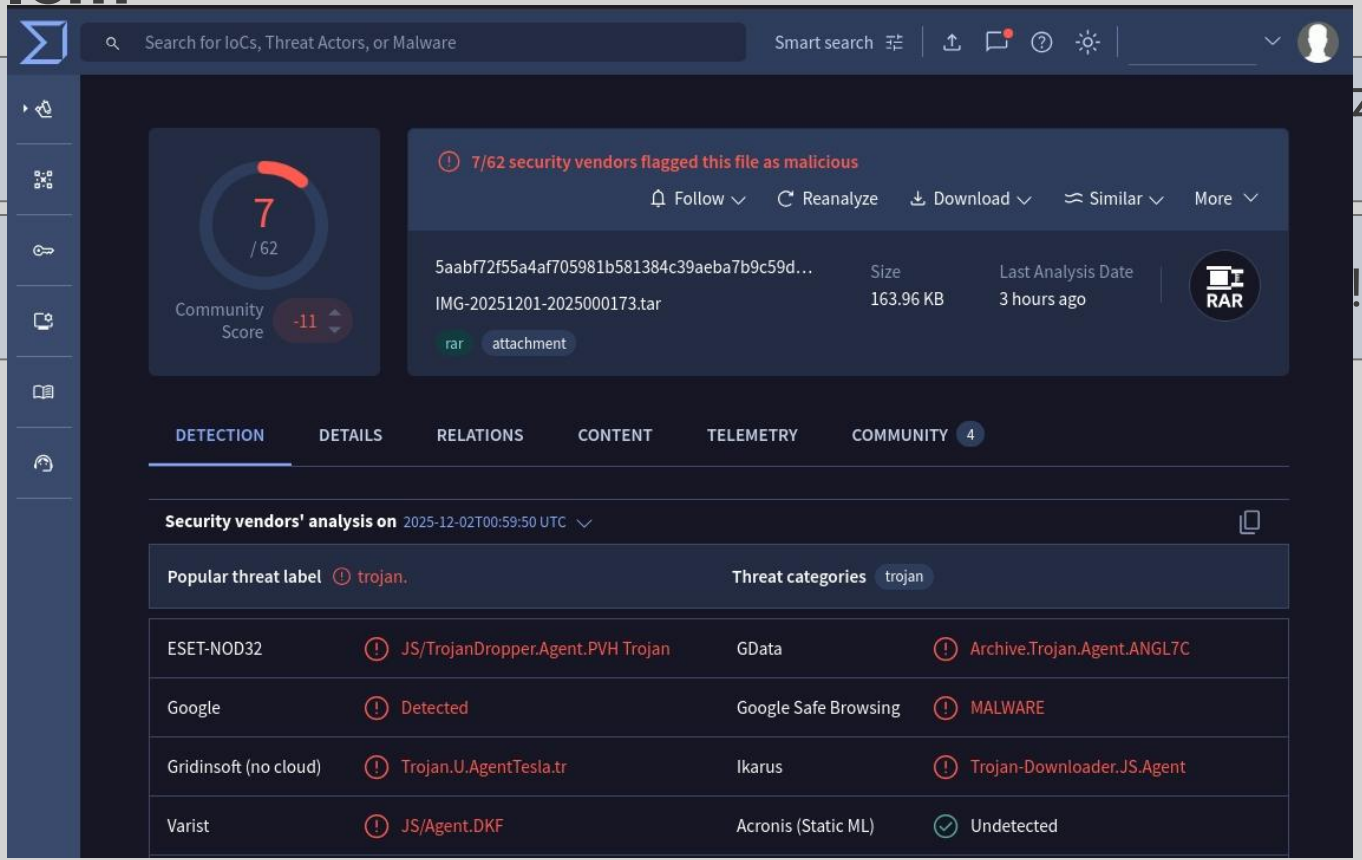
1 attachment: eFaktura nr F44556P0825SFAKAMC.docx 624 KB — Save

Problem

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

“Daj mi swój plik. Przeanalizuję go dla Ciebie za darmo!”

Problem



ziwnym

!”

Problem

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

“Daj mi swój plik. Przeanalizuję go dla Ciebie za darmo!”

“Nie rób tego! On chce Cię tylko wykorzystać!”

Problem

Filip Marczewski, OMH 2023

Problem

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

“Daj mi swój plik. Przeanalizuję go dla Ciebie za darmo!”

“Nie rób tego! On chce Cię tylko wykorzystać!”

“To co powinienem w takim razie zrobić?”

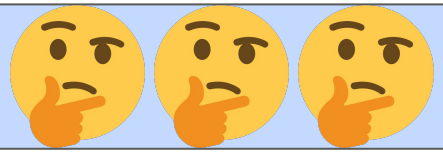
Problem

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

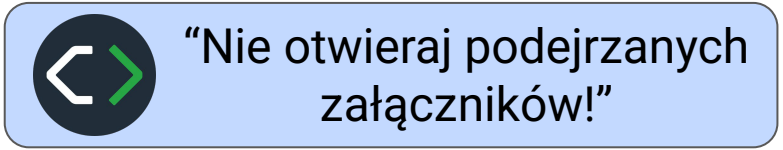
“Daj mi swój plik. Przeanalizuję go dla Ciebie za darmo!”

“Nie rób tego! On chce Cię tylko wykorzystać!”

“To co powinienem w takim razie zrobić?”

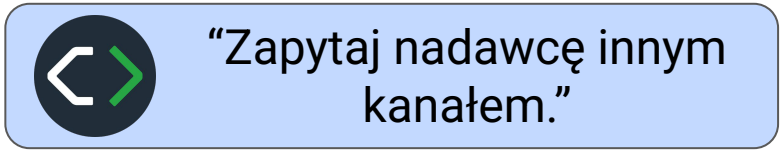


Problem (z rekomendacją)

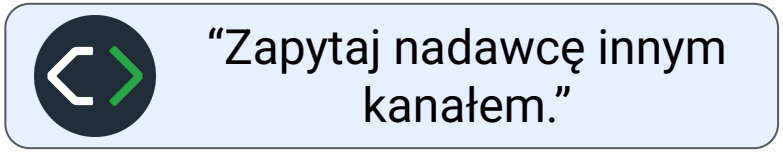


Problem (z rekomendacją)

Problem (z rekomendacją)



Problem (z rekomendacją)



Problem (z rekomendacją)

~~“Nie otwieraj podejrzanych załączników!”~~

“Zapytaj nadawcę innym kanałem.”

“Zgłoś incydent do CERTu?”

“Zgłoś do swojego działu bezpieczeństwa?”

Problem (z rekomendacją)

~~“Nie otwieraj podejrzanych załączników!”~~

“Zapytaj nadawcę innym kanałem.”

“Zgłoś incydent do CERTu?”

“Zgłoś do swojego działu bezpieczeństwa?”

“Wrzuć do firmowego sandboxa ale nie VirusTotala proszę!”

Problem (z rekomendacją)

~~“Nie otwieraj podejrzanych załączników!”~~

“Zapytaj nadawcę innym kanałem.”

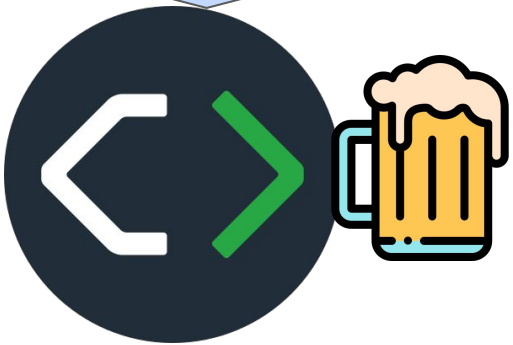
“Zgłoś incydent do CERTu?”

“Zgłoś do swojego działu bezpieczeństwa?”

“Wrzuć do firmowego sandboxa ale nie VirusTotala proszę!”

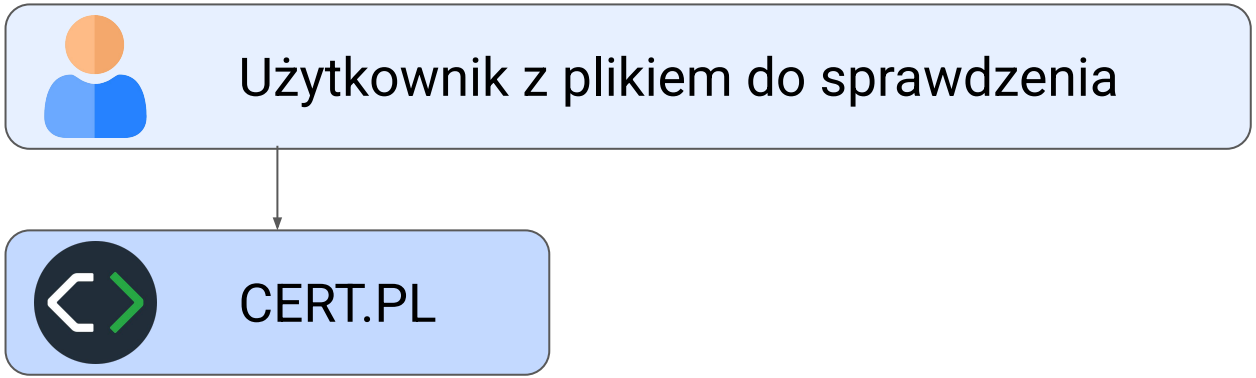
Problem (z rekomendacją)

W sumie czemu tego nie zrobić samemu?

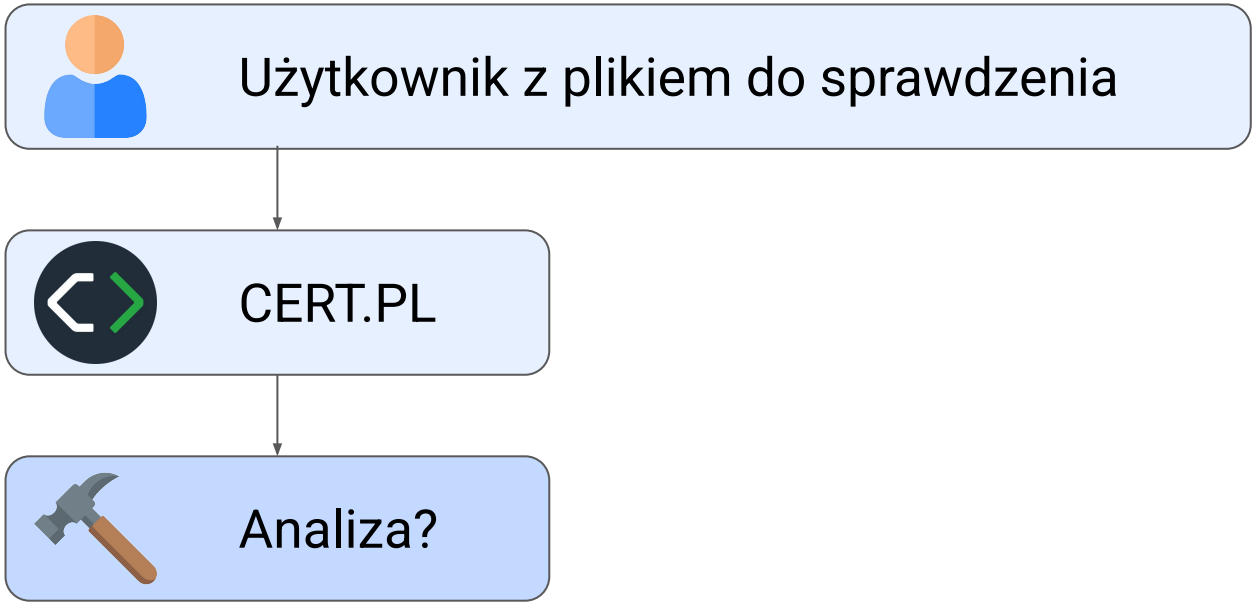


Pomysł

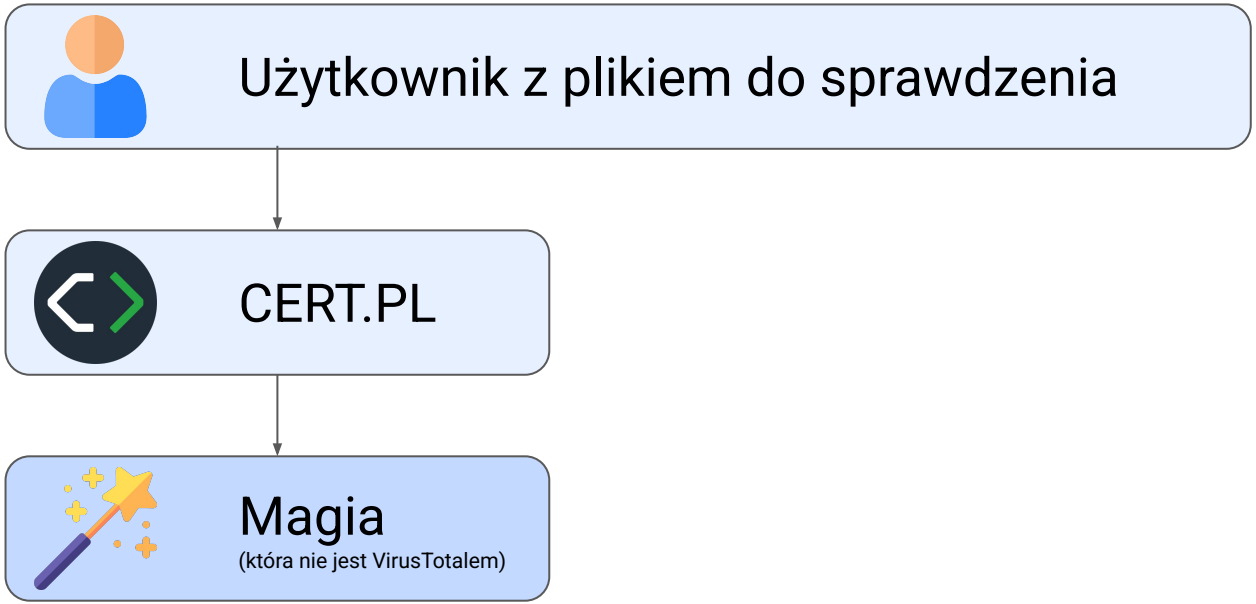
Pomysł



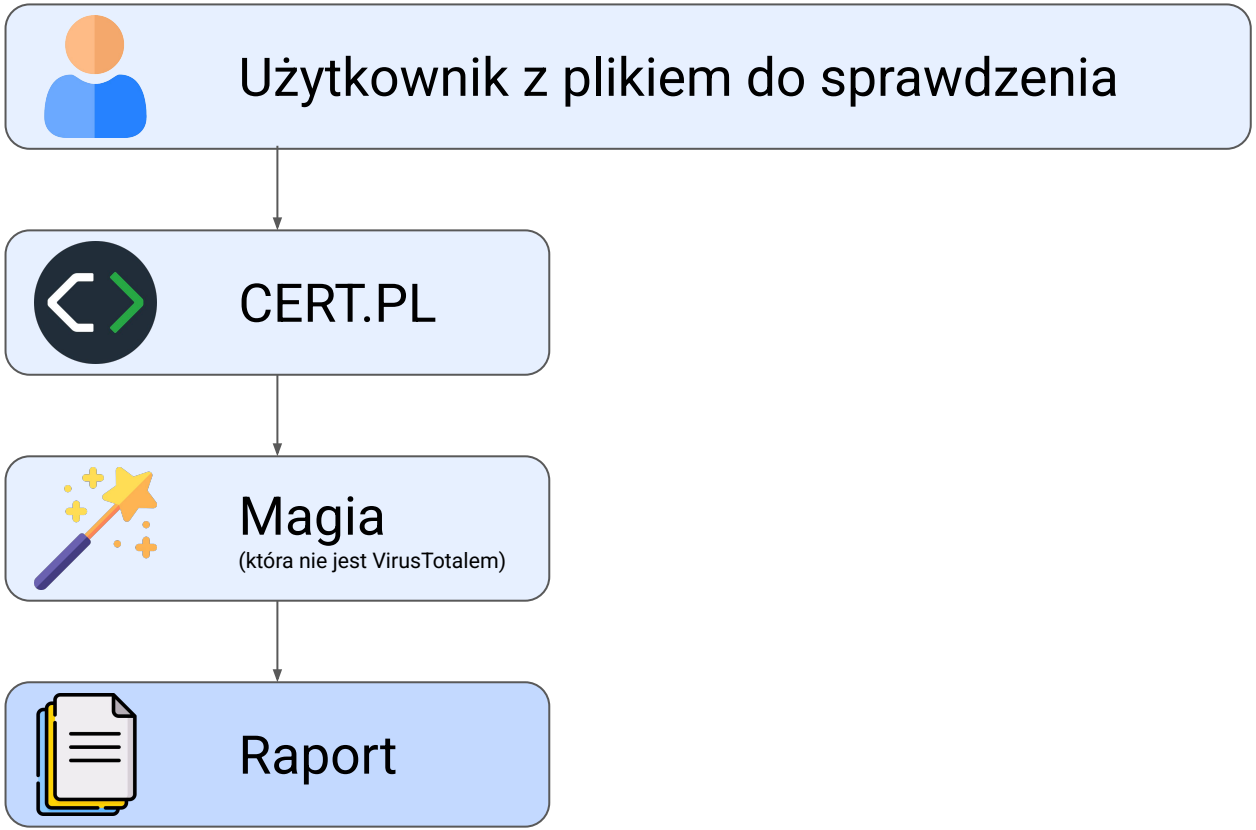
Pomysł



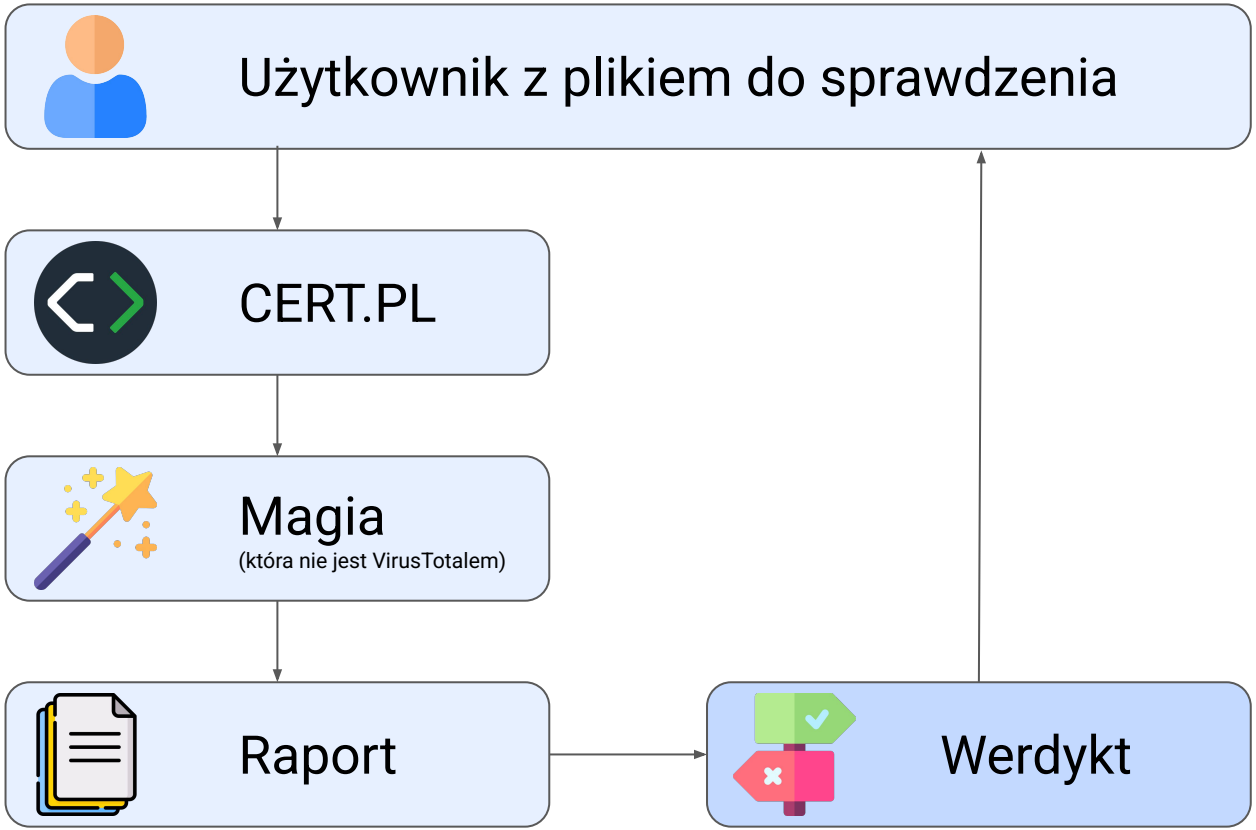
Pomysł


Użytkownik z plikiem do sprawdzenia
CERT.PL
Magia
(która nie jest VirusTotalem)

Pomysł


Użytkownik z plikiem do sprawdzenia
CERT.PL
Magia
(która nie jest VirusTotalem)
Raport

Pomysł


Użytkownik z plikiem do sprawdzenia
CERT.PL
Magia
(która nie jest VirusTotalem)
Raport
Werdykt

Nowe problemy

invoice.exe

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

invoice.exe

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

invoice.exe

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

invoice.exe

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

invoice.exe

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

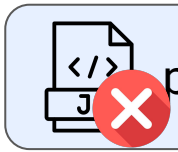
Kopia_patnosci.xls

Magia

(która nie jest VirusTotalem)

Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Kopia_patnosci.xls


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Kopia_patnosci.xls


FW_Umowa.eml


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Kopia_patnosci.xls


FW_Umowa.eml


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Kopia_patnosci.xls

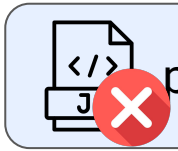

FW_Umowa.eml


kasia.png


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Kopia_patnosci.xls


FW_Umowa.eml


kasia.png


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

Kopia_patnosci.xls

FW_Umowa.eml

kasia.png

baza.sql.locky

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

Kopia_patnosci.xls

FW_Umowa.eml

kasia.png

baza.sql.locky

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

Kopia_patnosci.xls

FW_Umowa.eml

kasia.png

baza.sql.locky

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

Kopia_patnosci.xls

FW_Umowa.eml

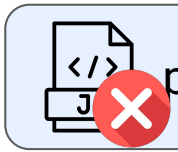
kasia.png

baza.sql.locky

Magia
(która nie jest VirusTotalem)

Werdykt

Nowe problemy


potwierdzenie.js


invoice.exe


Kopia_patnosci.xls


FW_Umowa.eml


kasia.png


baza.sql.locky


Magia
(która nie jest VirusTotalem)


Werdykt

Nowe problemy

potwierdzenie.js

invoice.exe

Kopia_patnosci.xls

FW_Umowa.eml

kasia.png

baza.sql.locky

Magia

(która nie jest VirusTotalem)

Werdykt

Publiczny interfejs

moje.cert.pl

mwdb.cert.pl

drakvuf sandbox

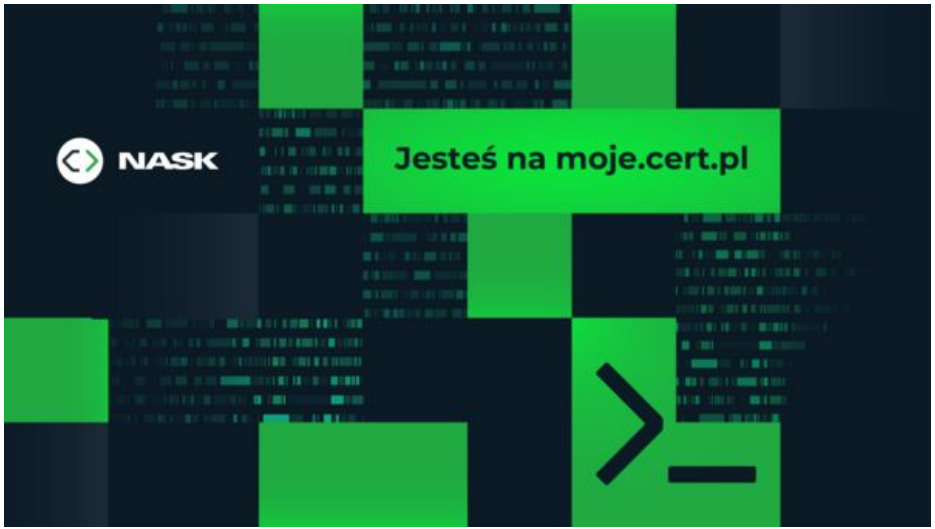
“system”

Publiczny interfejs

moje.cert.pl

Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

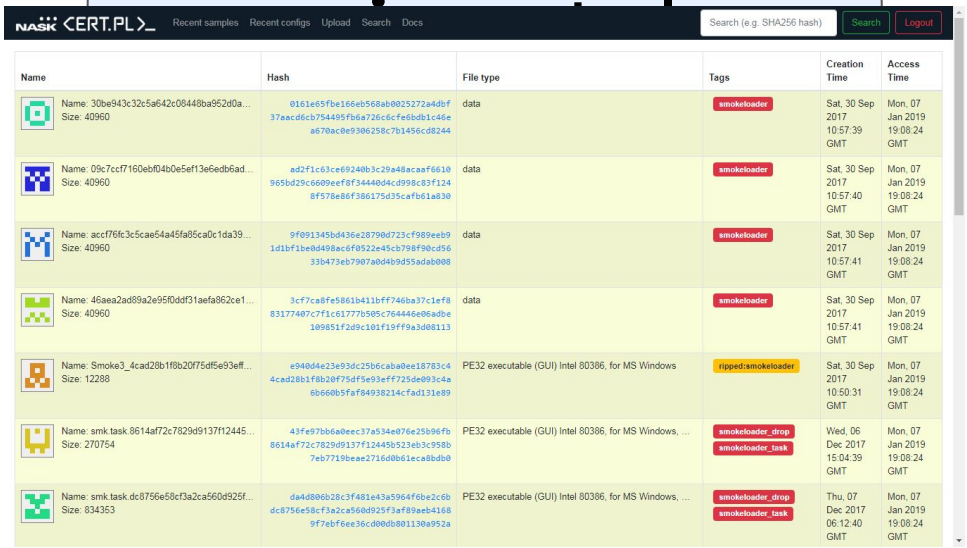


Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl

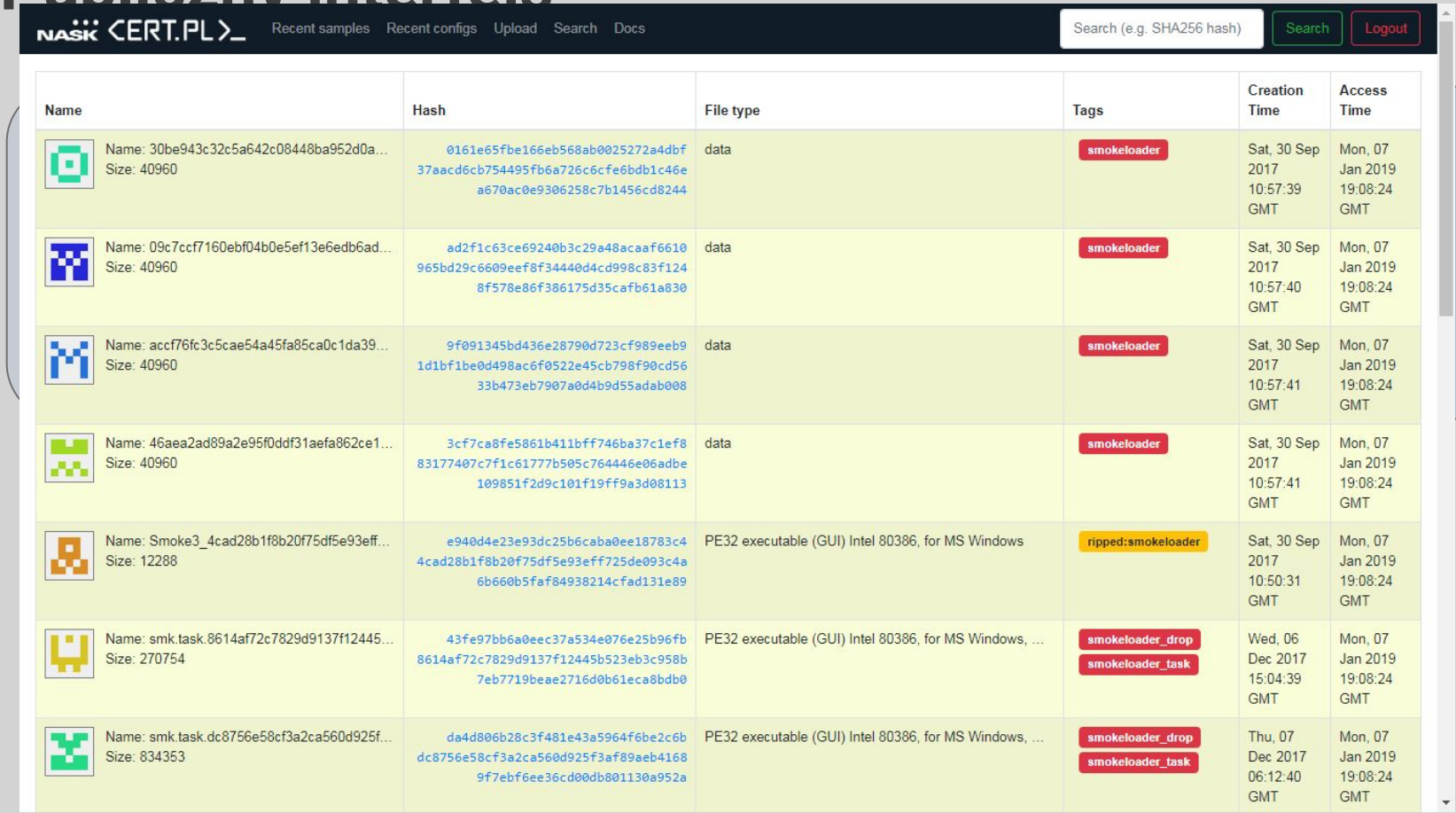
Publiczny interfejs



mwdb.cert.pl

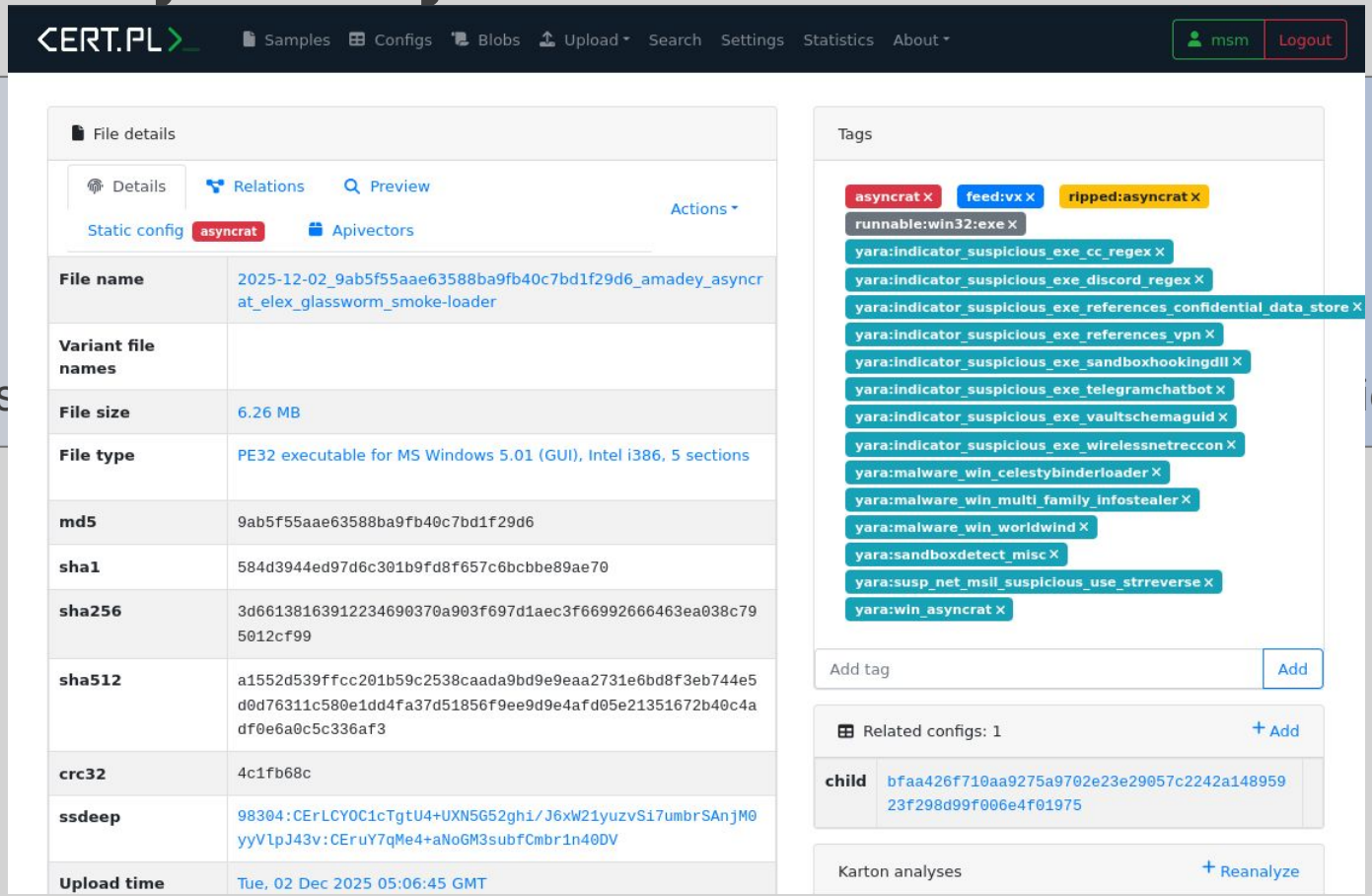
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

Publiczny interfejs



Name	Hash	File type	Tags	Creation Time	Access Time
Name: 30be943c32c5a642c08448ba952d0a... Size: 40960	0161e65fbe166eb568ab0025272a4dbf37aacd6cb754495fb6a726c6cfe6bdb1c46ea670ac0e9306258c7b1456cd8244	data	smokeloader	Sat, 30 Sep 2017 10:57:39 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: 09c7ccf7160ebf04b0e5ef13e6edb6ad... Size: 40960	ad2f1c63ce69240b3c29a48acaaf6610965bd29c6609eef8f34440d4cd998c83f1248f578e86f386175d35cafb61a830	data	smokeloader	Sat, 30 Sep 2017 10:57:40 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: accf76fc3c5cae54a45fa85ca0c1da39... Size: 40960	9f091345bd436e28790d723cf989eeb91d1bf1be0d498ac6f0522e45cb798f90cd5633b473eb7907a0d4b9d55adab008	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: 46aea2ad89a2e95f0ddf31aefa862ce1... Size: 40960	3cf7ca8fe5861b411bff746ba37c1ef883177407c7f1c61777b505c764446e06adbe109851f2d9c101f19ff9a3d08113	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: Smoke3_4cad28b1f8b20f75df5e93eff... Size: 12288	e940d4e23e93dc25b6caba0ee18783c44cad28b1f8b20f75df5e93eff725de093c4a6b660b5faf84938214cfad131e89	PE32 executable (GUI) Intel 80386, for MS Windows	ripped:smokeloader	Sat, 30 Sep 2017 10:50:31 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: smk.task.8614af72c7829d9137f12445... Size: 270754	43fe97bb6a0eec37a534e076e25b96fb8614af72c7829d9137f12445b523eb3c958b7eb7719beae2716d0b61eca8bdb0	PE32 executable (GUI) Intel 80386, for MS Windows, ...	smokeloader_drop smokeloader_task	Wed, 06 Dec 2017 15:04:39 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: smk.task.dc8756e58cf3a2ca560d925f... Size: 834353	da4d806b28c3f481e43a5964f6be2c6bdc8756e58cf3a2ca560d925f3af89aeb41689f7ebf6ee36cd00db801130a952a	PE32 executable (GUI) Intel 80386, for MS Windows, ...	smokeloader_drop smokeloader_task	Thu, 07 Dec 2017 06:12:40 GMT	Mon, 07 Jan 2019 19:08:24 GMT

Publiczny interfejs



Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

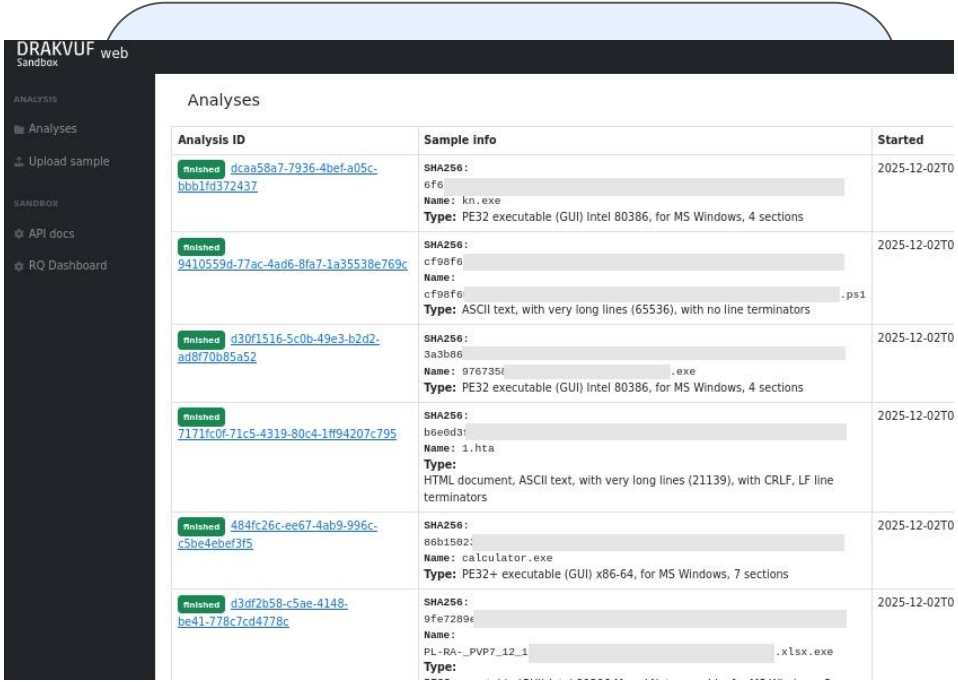
mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox

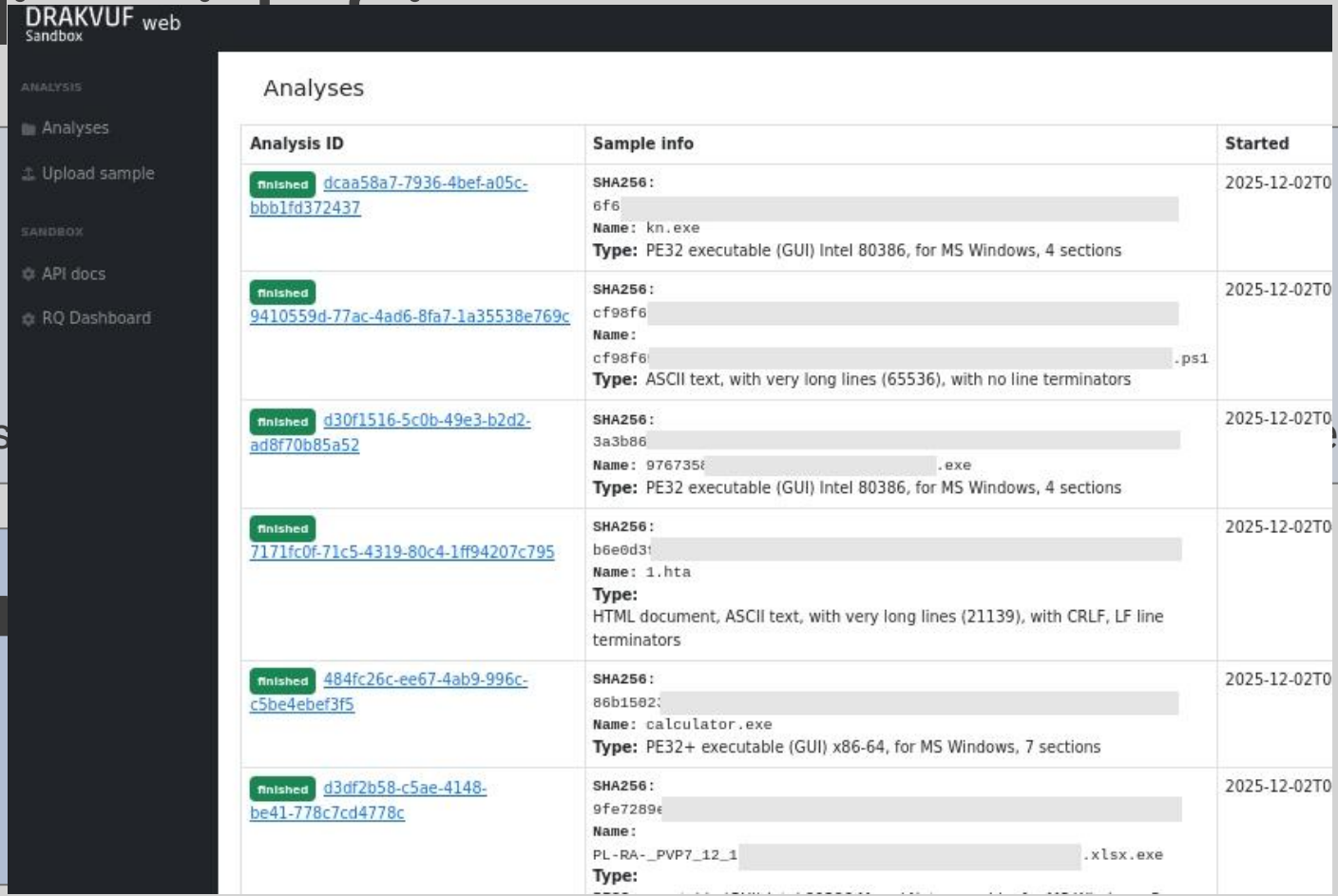
Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

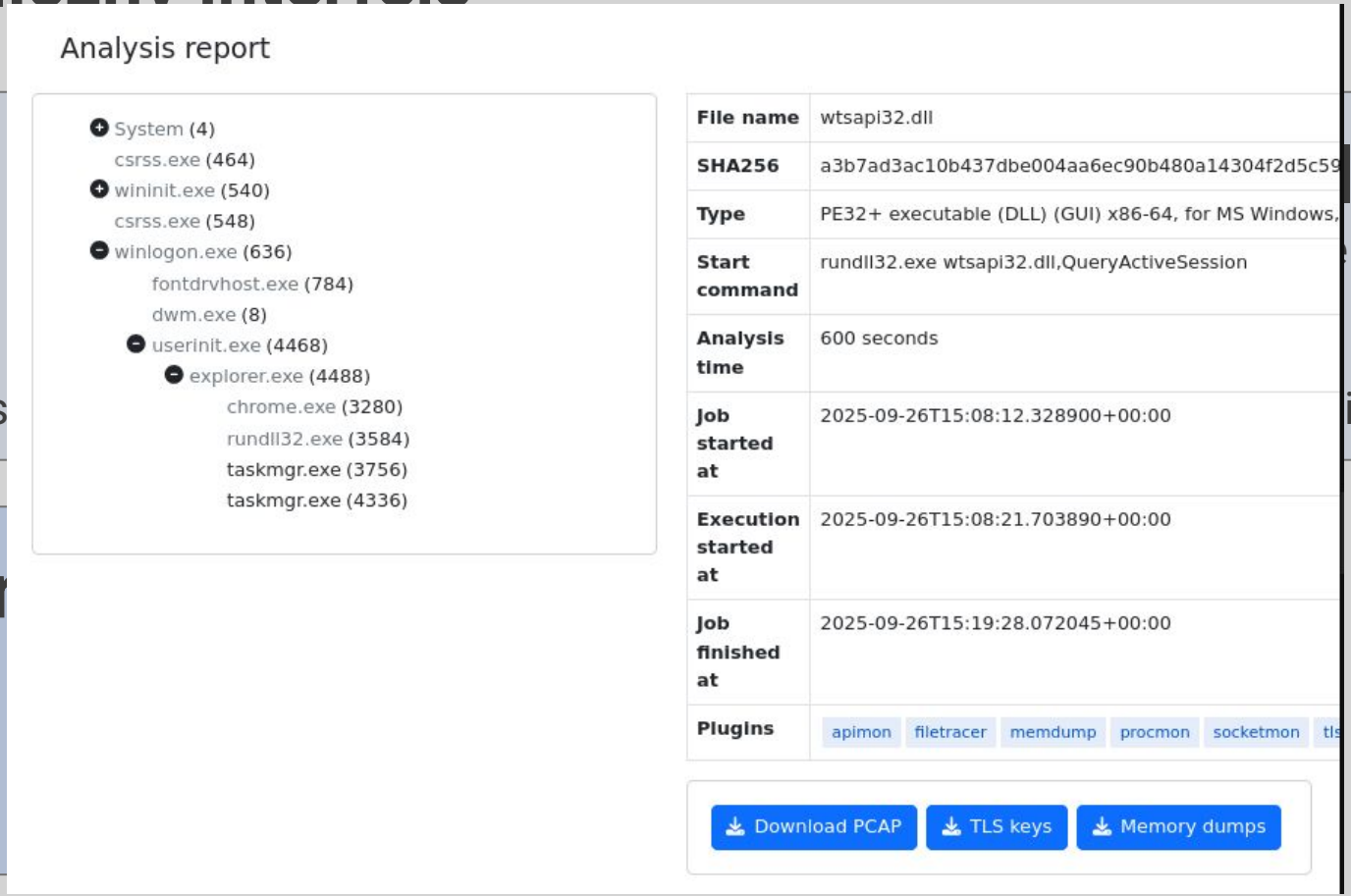
drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza



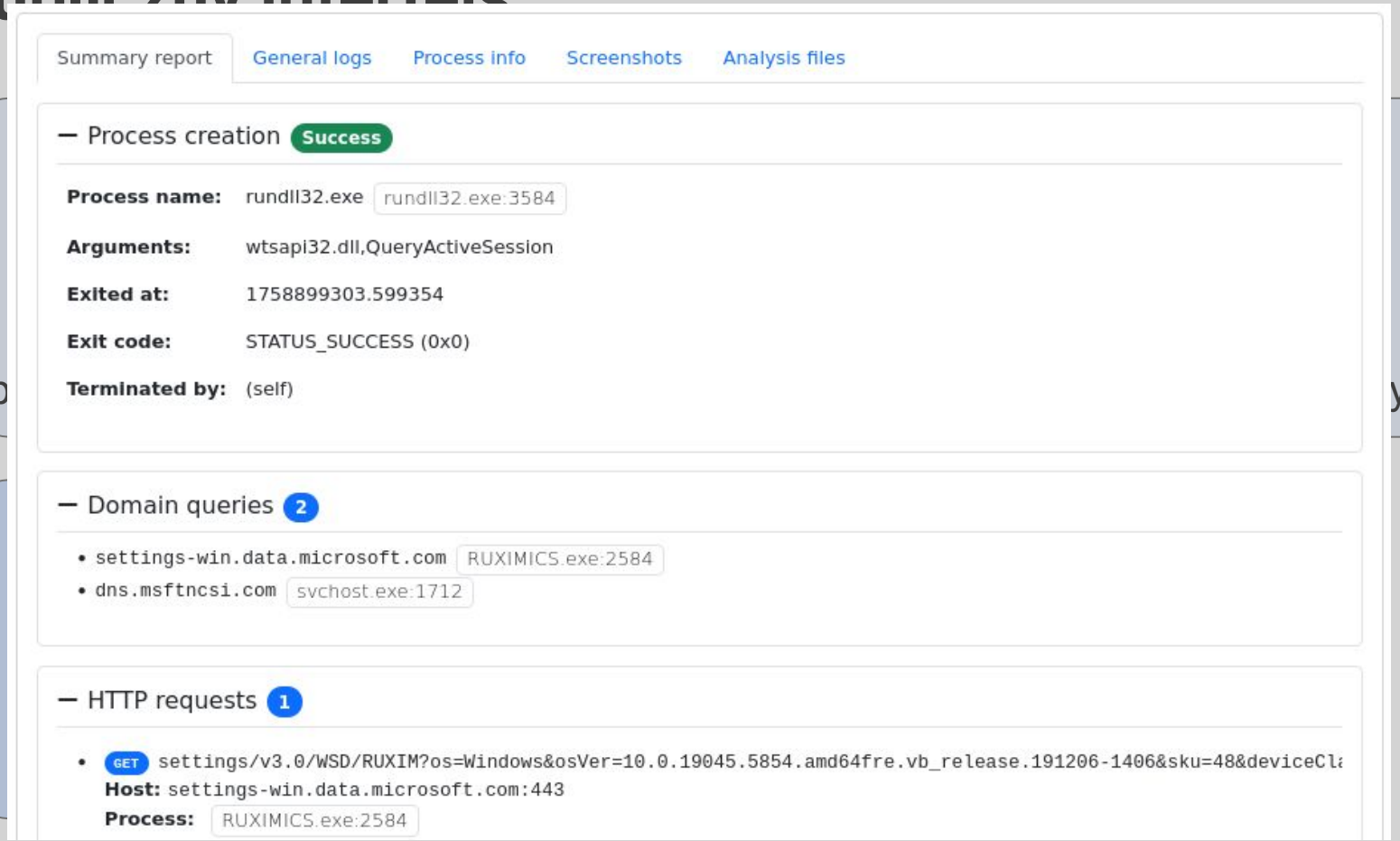
Publ


DRAKVUF web
Sandbox
ANALYSIS
Analyses
Upload sample
SANDBOX
API docs
RQ Dashboard
Analyses
Analysis ID
Sample info
Started
finished dcaa58a7-7936-4bef-a05c-bbb1fd372437
SHA256:
6f6
Name: kn.exe
Type: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
2025-12-02T0
finished 9410559d-77ac-4ad6-8fa7-1a35538e769c
SHA256:
cf98f6
Name:
cf98f6
.ps1
Type: ASCII text, with very long lines (65536), with no line terminators
2025-12-02T0
finished d30f1516-5c0b-49e3-b2d2-ad8f70b85a52
SHA256:
3a3b86
Name: 976735
.exe
Type: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
2025-12-02T0
finished 7171fc0f-71c5-4319-80c4-1ff94207c795
SHA256:
b6e0d3
Name: 1.hta
Type:
HTML document, ASCII text, with very long lines (21139), with CRLF, LF line terminators
2025-12-02T0
finished 484fc26c-ee67-4ab9-996c-c5be4ebef3f5
SHA256:
86b1502
Name: calculator.exe
Type: PE32+ executable (GUI) x86-64, for MS Windows, 7 sections
2025-12-02T0
finished d3df2b58-c5ae-4148-be41-778c7cd4778c
SHA256:
9fe7289
Name:
PL-RA-_PVP7_12_1
.xlsx.exe
Type:
2025-12-02T0

Publicznv interfeis



Publiczny interfejs



Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”

Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”
“**oceniacz złośliwości**”

Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”
“oceniacz złośliwości”
dla “zwykłych ludzi”

Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”
“oceniacz złośliwości”
dla “zwykłych ludzi”
dostępny publicznie

Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”
“oceniacz złośliwości”
dla “zwykłych ludzi”
dostępny publicznie
nie wymaga bycia technicznym

Publiczny interfejs

moje.cert.pl
usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

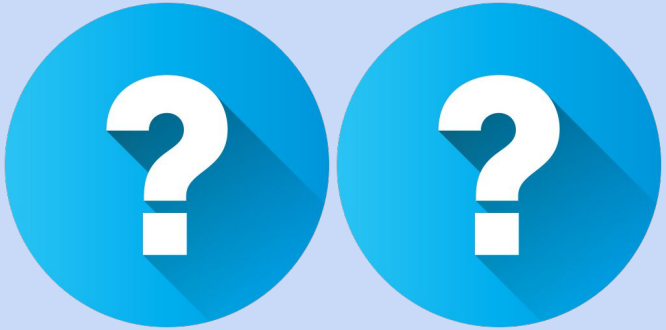
mwdb.cert.pl
repozytorium malware
dla researcherów
invite only
wymaga specjalistycznej wiedzy

drakvuf sandbox
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”
“oceniacz złośliwości”
dla “zwykłych ludzi”
dostępny **przez moje.cert.pl**
nie wymaga bycia technicznym

Część 2

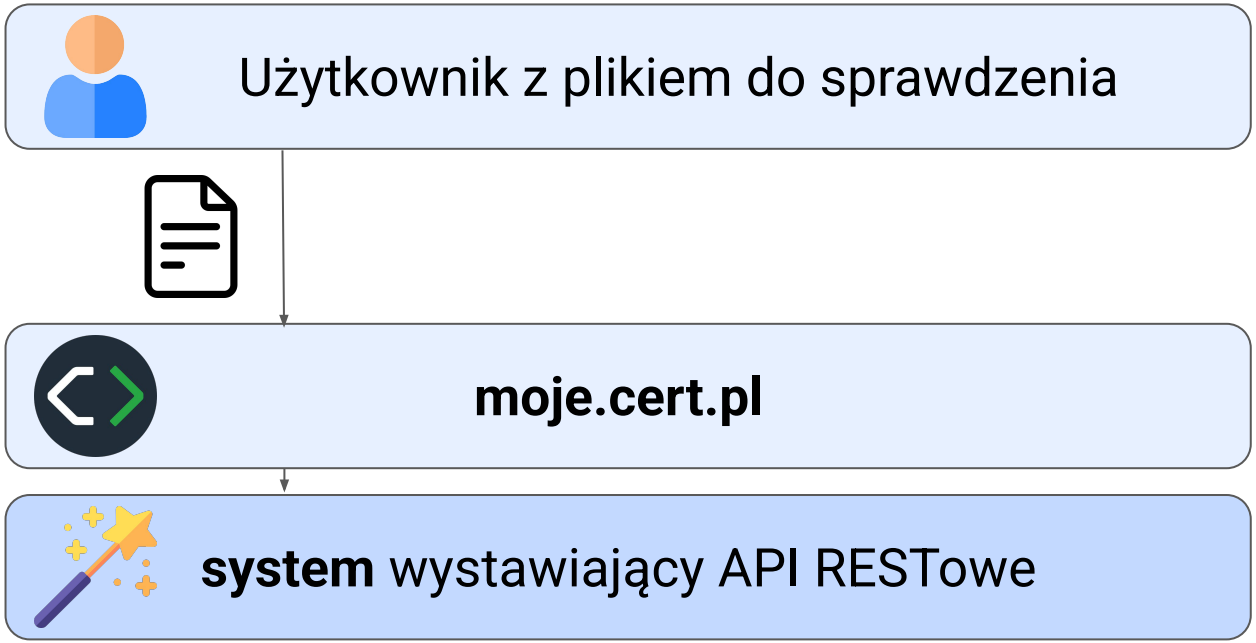
Jak go chcemy rozwiązać?



Po pierwsze: API

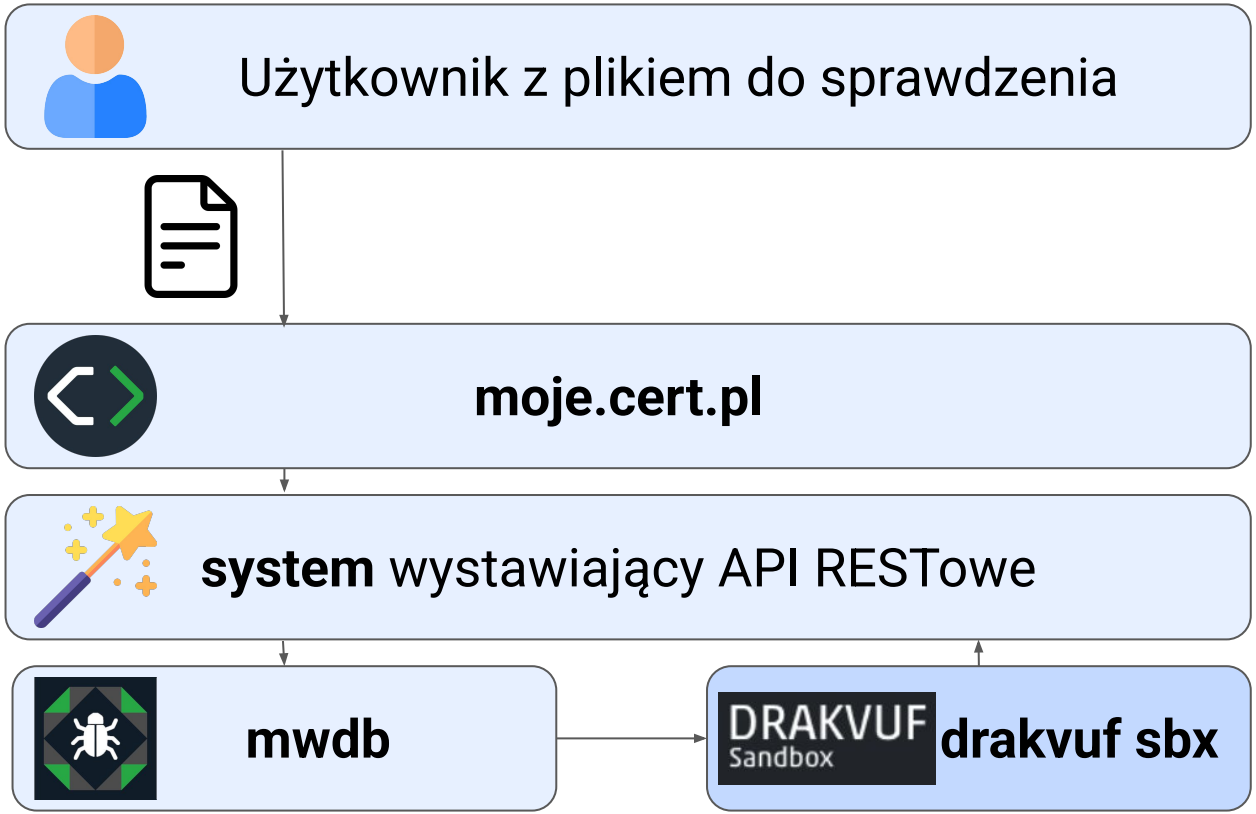
Po pierwsze: API

Po pierwsze: API

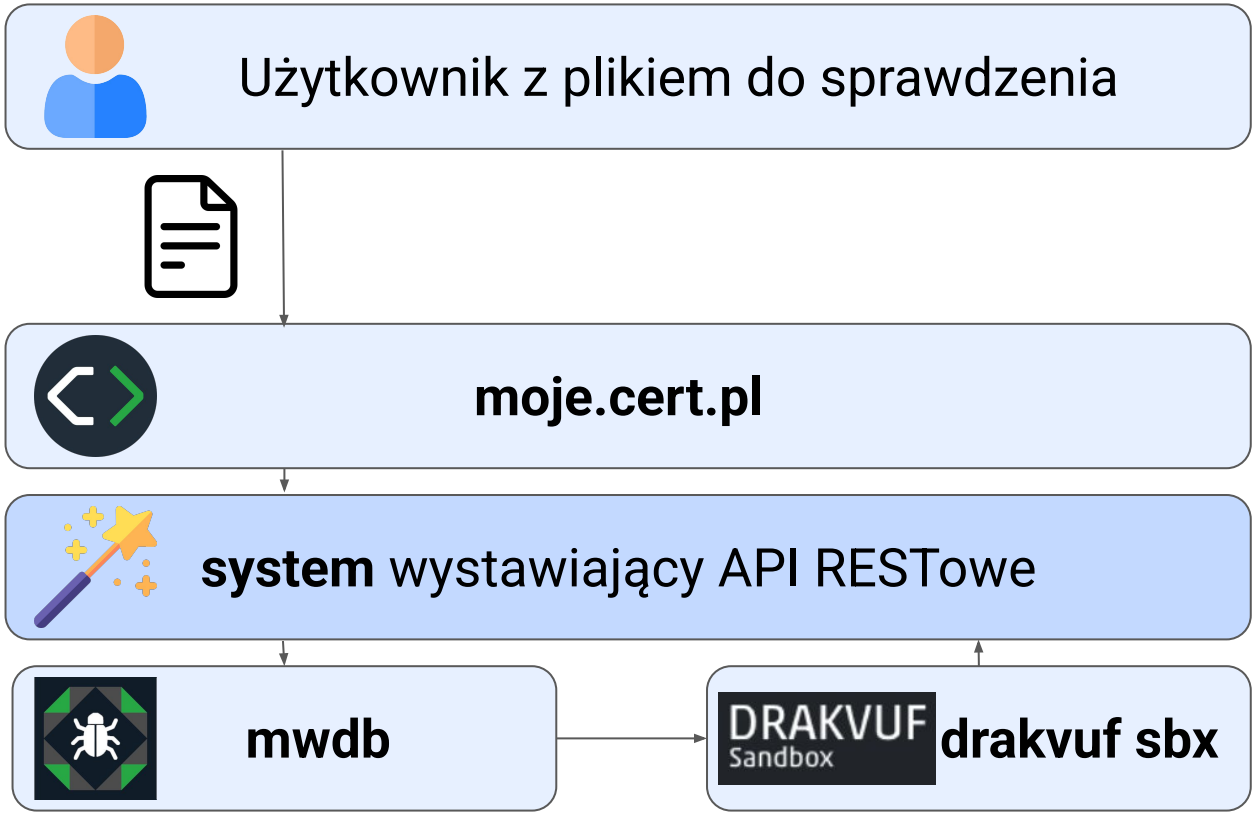


Po pierwsze: API

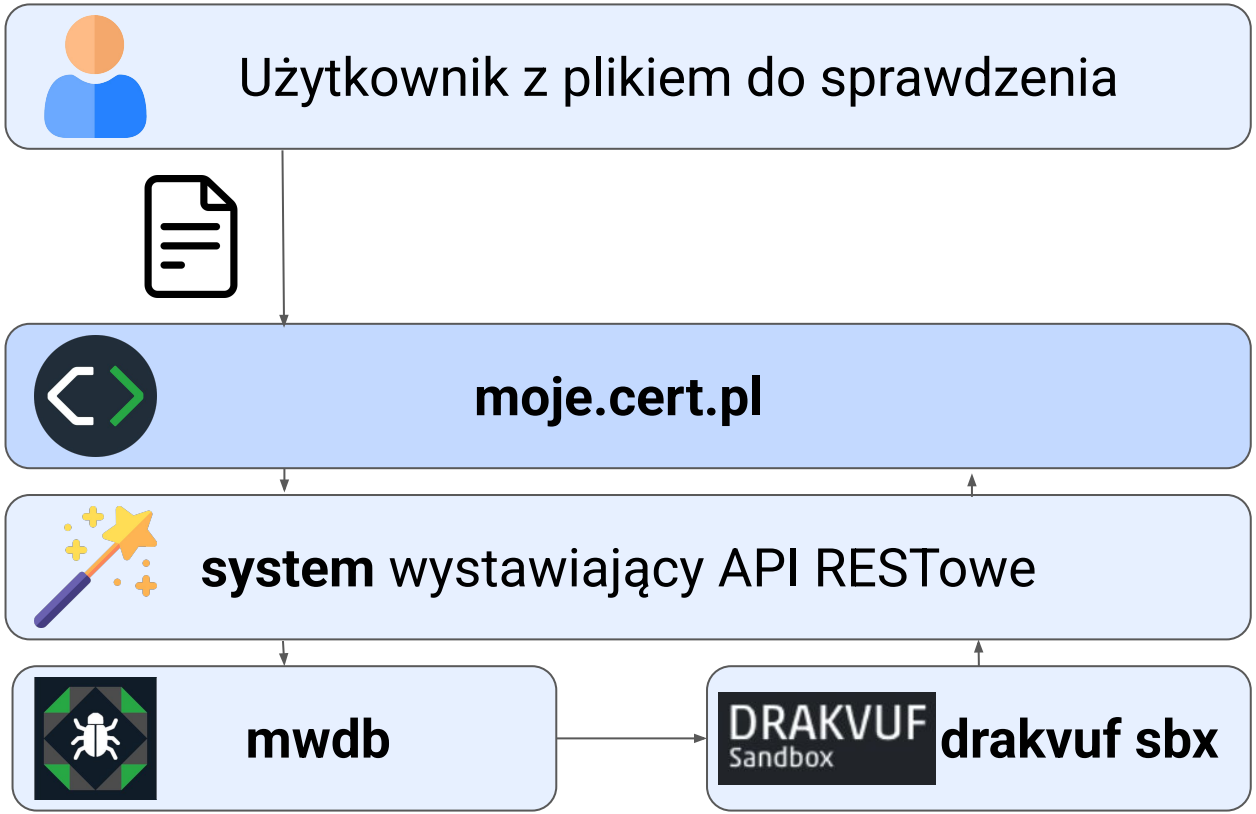
Po pierwsze: API



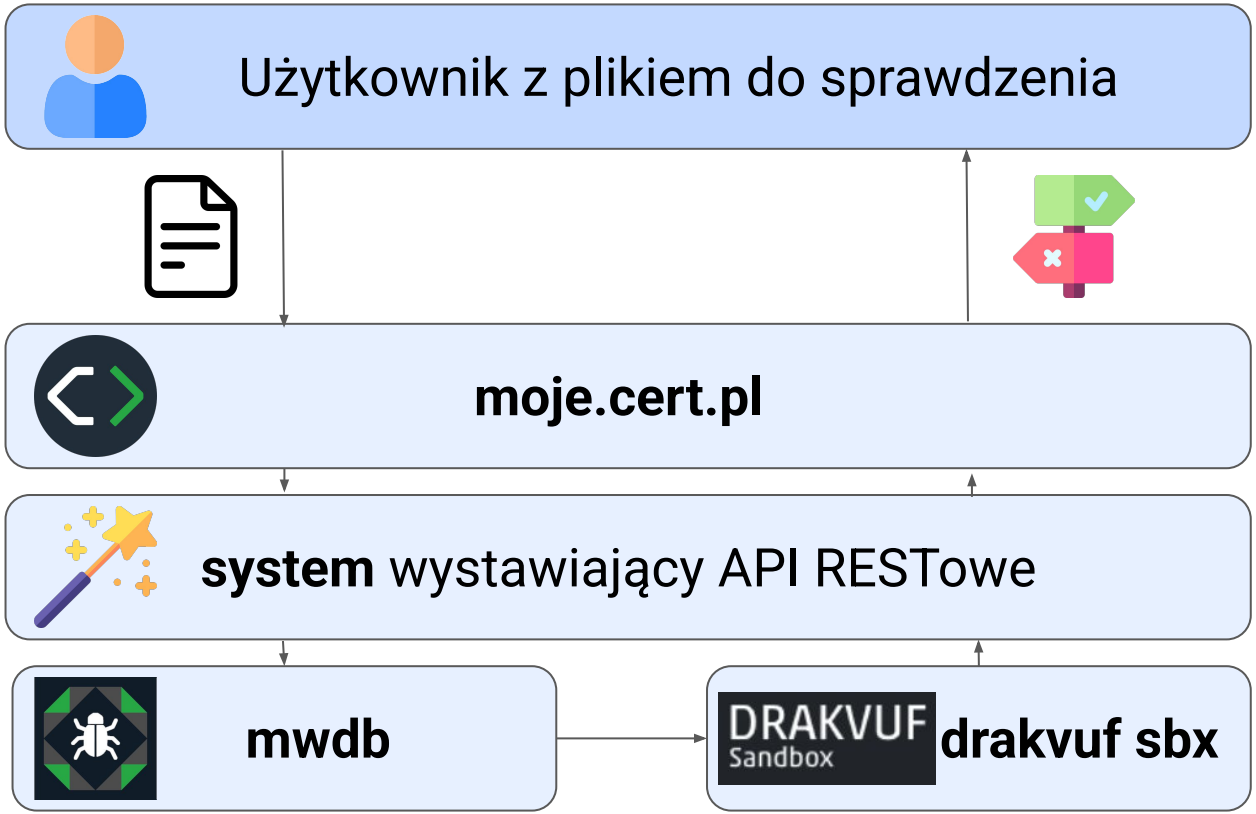
Po pierwsze: API



Po pierwsze: API



Po pierwsze: API



Silnik analityczny

Silnik analityczny

system
(który nie jest VirusTotalem)

mwdb signatures
wszystkie dane
powiązane do pliku:
nazwy plików,
tagi,
atrybuty.

Silnik analityczny

system
(który nie jest VirusTotalem)

mwdb signatures
wszystkie dane
powiązane do pliku:
nazwy plików,
tagi,
atrybuty.

Tags

ripped:agenttesla ✕ runnable:win32:exe ✕
yara:win_agent_tesla ✕

Family	xworm
Config type	static
+ ChatID	7588932713
+ Group	XWorm V6.5 by c3lestial.fun
+ Hosts	needs-developed.gl.at.ply.gg
+ InstallDir	%AppData%
+ InstallStr	XWormClient.exe

Silnik analityczny

system
(który nie jest VirusTotalem)

mwdb signatures
wszystkie dane powiązane do pliku:
nazwy plików,
tagi,
atrybuty.

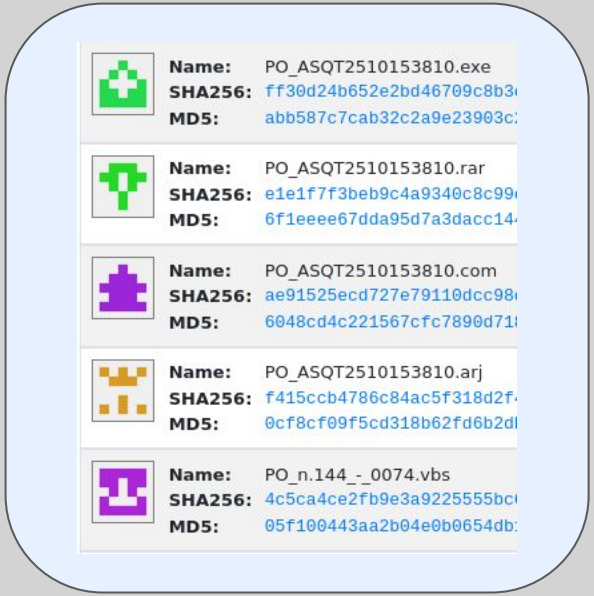
custom signatures
reguły specyficzne dla typu pliku:
docx generujący HTTP,
autoit ładujący DLL,
HTML z polem na hasło.

Silnik analityczny

system
(który nie jest VirusTotalem)

mwdb signatures
wszystkie dane
powiązane do pliku:
nazwy plików,
tagi,
atrybuty.

custom signatures
reguły specyficzne dla
typu pliku:
docx generujący HTTP,
autoit ładujący DLL,
HTML z polem na hasło.



Silnik analityczny

system
(który nie jest VirusTotalem)

mwdb signatures
wszystkie dane powiązane do pliku:
nazwy plików,
tagi,
atrybuty.

custom signatures
reguły specyficzne dla typu pliku:
docx generujący HTTP,
autoit ładujący DLL,
HTML z polem na hasło.

recursive signatures
reguły zależne od powiązanych IoC

Silnik analityczny

mwdb

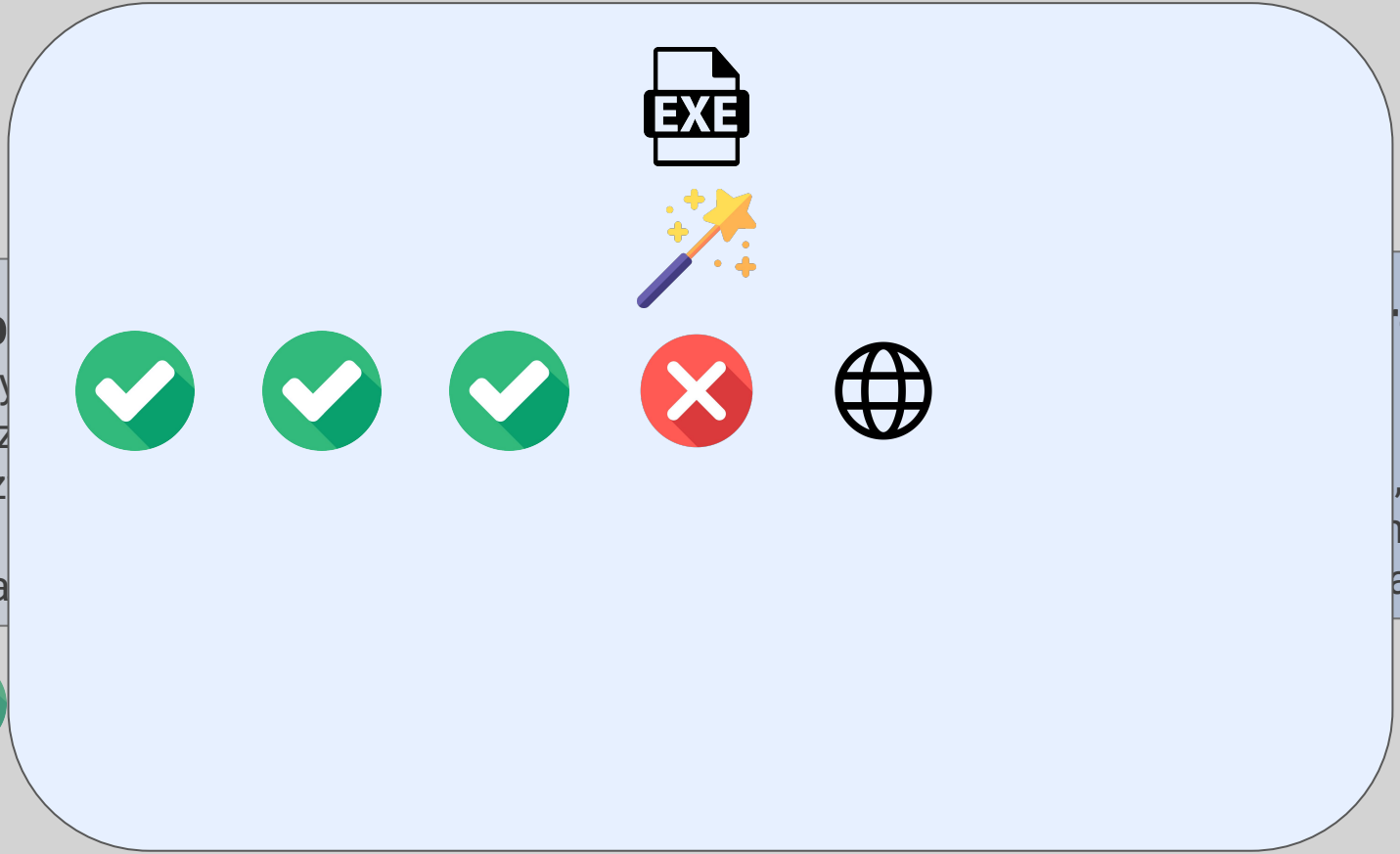
wszy
powiąz
naz

a

res

,
ngu,
are.

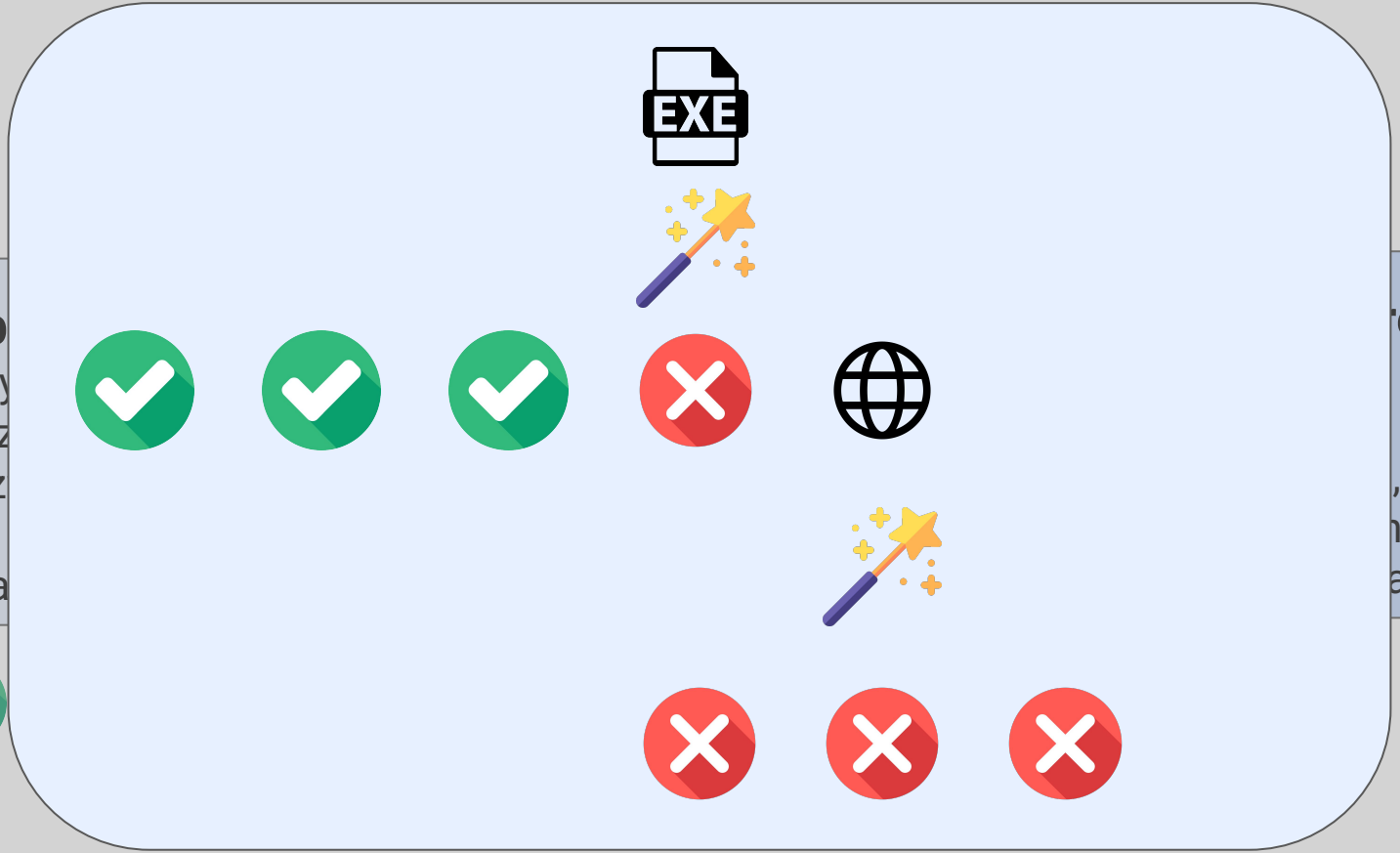
Silnik analityczny



mwdb
wszy
powiąz
naz
a

res
,
ngu,
are.

Silnik analityczny



Silnik analityczny

system
(który nie jest VirusTotalem)

mwdb signatures
wszystkie dane powiązane do pliku:
nazwy plików,
tagi,
atrybuty.

custom signatures
reguły specyficzne dla typu pliku:
docx generujący HTTP,
autoit ładujący DLL,
HTML z polem na hasło.

recursive signatures
reguły zależne od powiązanych IoC:
ruch do znanego C2,
link do znanego phishingu,
pobrano na dysk malware.

Werdykt

Werdykt

Podejrzana nazwa: 3/10😈
Używa CryptoApi: 4/10😈
Enkoduje XORem: 3/10😈

Werdykt

Podejrzana nazwa: 3/10😈
Używa CryptoApi: 4/10😈
Enkoduje XORem: 3/10😈

3 + 4 + 3 = 10/10😈

Werdykt

Podejrzana nazwa: 3/10😈
Używa CryptoApi: 4/10😈
Enkoduje XORem: 3/10😈

Signed by Microsoft: 0/10😈

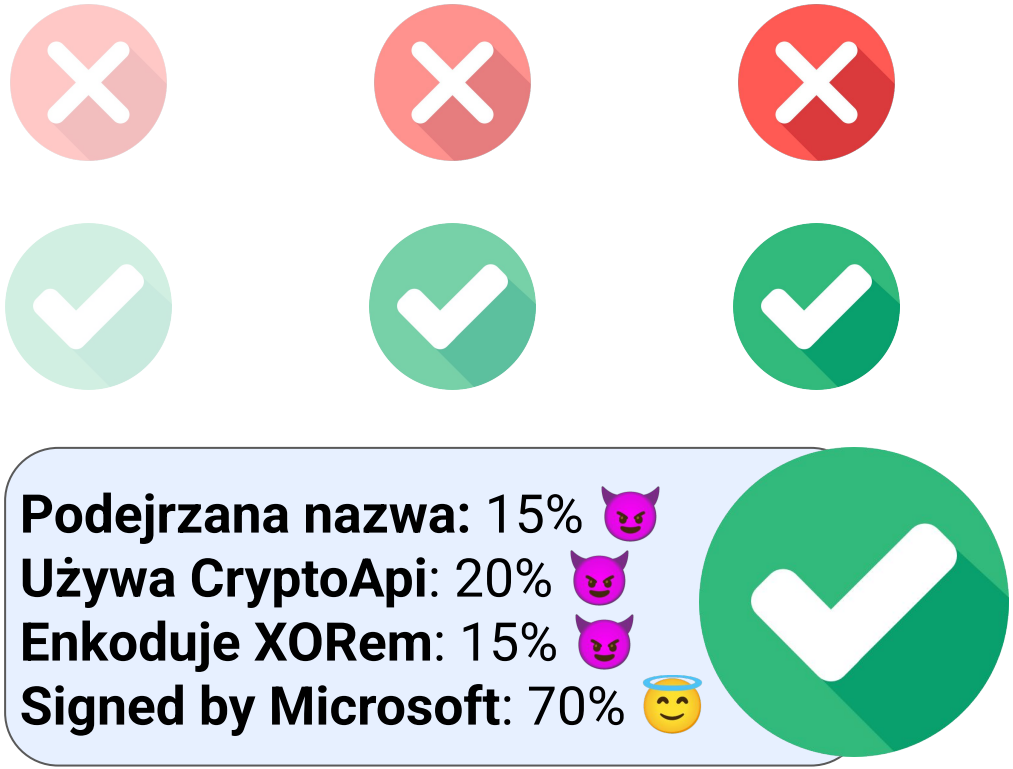
Werdykt


Podejrzana nazwa: 15% 😈
Używa CryptoApi: 20% 😈
Enkoduje XORem: 15% 😈

Werdykt

Podejrzana nazwa: 15% 😈
Używa CryptoApi: 20% 😈
Enkoduje XORem: 15% 😈
Signed by Microsoft: 70% 😇

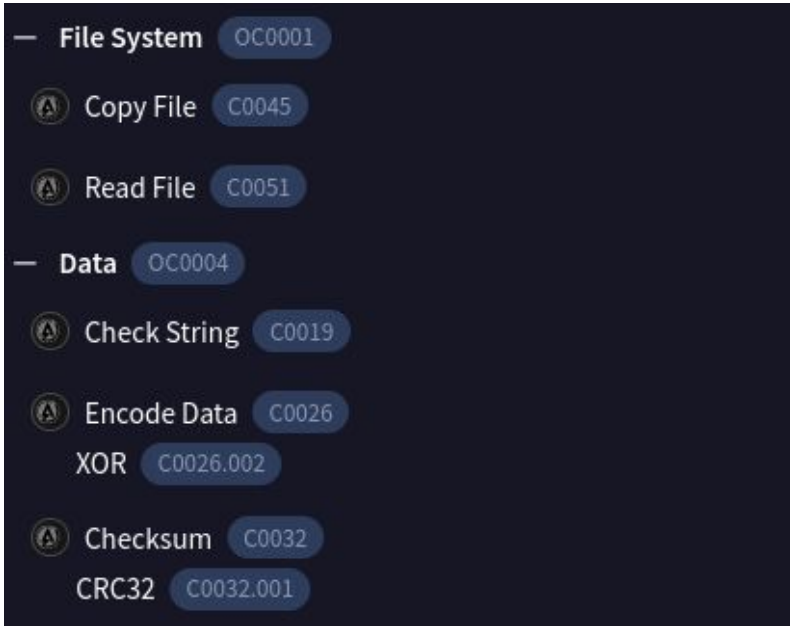
Werdykt

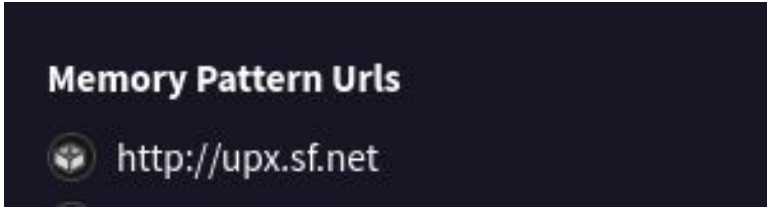

Podejrzana nazwa: 15% 😈
Używa CryptoApi: 20% 😈
Enkoduje XORem: 15% 😈
Signed by Microsoft: 70% 😇

Werdykt

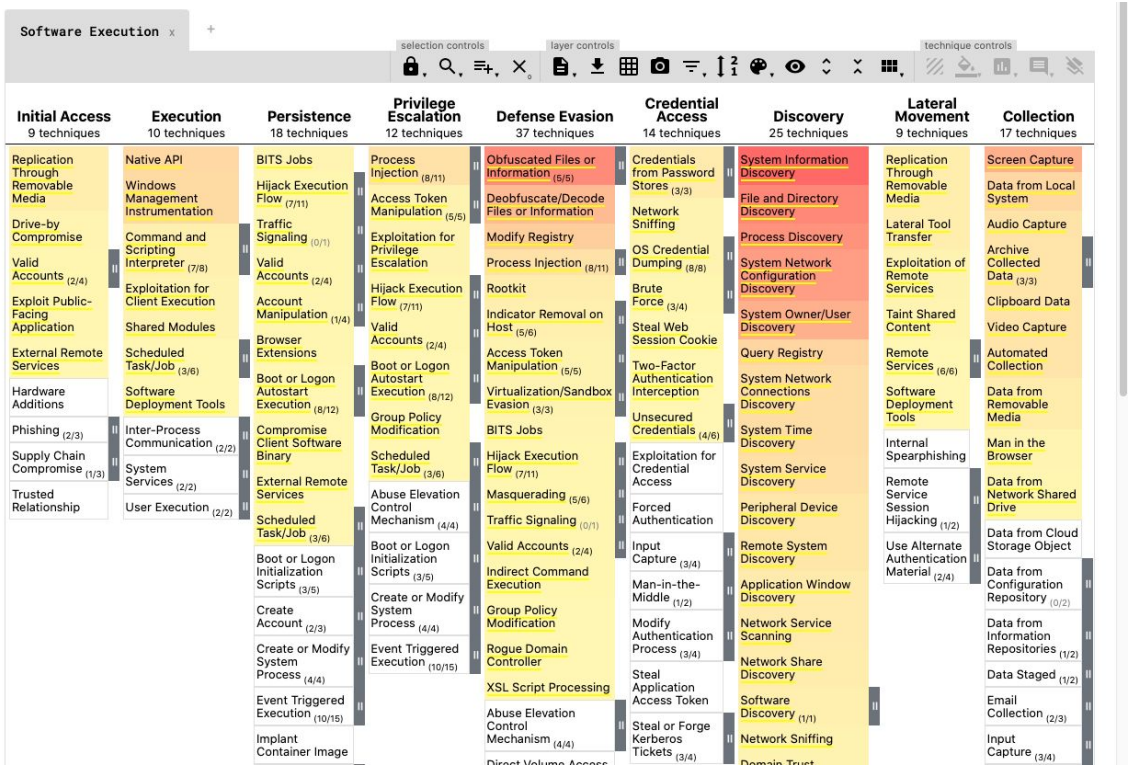
Indykatory


Malware Behavior Catalog Tree
Anti-Static Analysis OB0002
Obfuscated Files or Information E1027
Encoding - Standard Algorithm E1027.m02
Defense Evasion OB0006
Obfuscated Files or Information E1027
Encoding - Standard Algorithm E1027.m02
Discovery OB0007
File and Directory Discovery E1083


File System OC0001
Copy File C0045
Read File C0051
Data OC0004
Check String C0019
Encode Data C0026
XOR C0026.002
Checksum C0032
CRC32 C0032.001


Memory Pattern Urls
http://upx.sf.net

Indykatory



T1059.003
(Windows Command Shell)

T1555.003
(Credentials from Web Browsers)

Indykatory

Website | Download | Web Interface

---

capa detects capabilities in executable files. You run it against a PE, ELF, .NET module, shellcode file, or a sandbox report and it tells you what it thinks the program can do. For example, it might suggest that the file is a backdoor, is capable of installing services, or relies on HTTP to communicate.

To interactively inspect capa results in your browser use the capa Explorer Web.

If you want to inspect or write capa rules, head on over to the capa-rules repository. Otherwise, keep reading.

Below you find a list of our capa blog posts with more details.

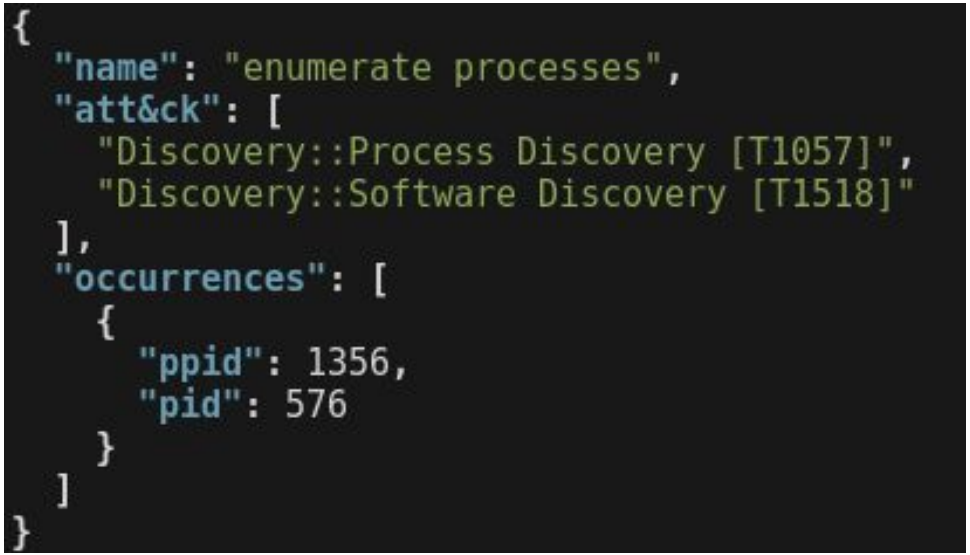
Indykatory

```
$ capa.exe suspicious.exe

+--------------------+-------------------------------------------------------------------------+
| ATT&CK Tactic      | ATT&CK Technique                                                        |
|--------------------+-------------------------------------------------------------------------|
| DEFENSE EVASION    | Obfuscated Files or Information [T1027]                                 |
| DISCOVERY          | Query Registry [T1012]                                                  |
|                    | System Information Discovery [T1082]                                   |
| EXECUTION          | Command and Scripting Interpreter::Windows Command Shell [T1059.003]    |
|                    | Shared Modules [T1129]                                                  |
| EXFILTRATION       | Exfiltration Over C2 Channel [T1041]                                    |
| PERSISTENCE        | Create or Modify System Process::Windows Service [T1543.003]            |
+--------------------+-------------------------------------------------------------------------+

+-----------------------------------------+-----------------------------------------------+
| CAPABILITY                              | NAMESPACE                                     |
|-----------------------------------------+-----------------------------------------------|
| read and send data from client to server | c2/file-transfer                             |
| execute shell command and capture output | c2/shell                                     |
| receive data (2 matches)                | communication                                 |
| send data (6 matches)                   | communication                                 |
| connect to HTTP server (3 matches)      | communication/http/client                     |
| send HTTP request (3 matches)           | communication/http/client                     |
| create pipe                             | communication/named-pipe/create               |
```

Indykatory



2024 Program | The Honeynet Project

Contributor

Yacine Elhamer

View Code

Extending the DRAKVUF Sandbox analytic pipeline

Mentors	Organization
Jarosław Jedynak	The Honeynet Project

Część 3

Co nam (i Wam) to da?

Żywotne potrzeby społeczeństwa

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

Żywotne potrzeby społeczeństwa

“Hmm, na mój e-mail pracowy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”

1. Zapotrzebowanie w constituency

Prior art

“system”

“oceniacz złośliwości”
dla każdego
dostępny publicznie
nie wymaga bycia technicznym

Prior art

Antywirus?

“oceniacz złośliwości”
dla każdego
dostępny publicznie
nie wymaga bycia technicznym

Prior art

Antywirus?

“oceniacz złośliwości”
dla każdego
dostępny publicznie
nie wymaga bycia technicznym

Inny Antywirus

Prior art

Inny Antywirus

Antywirus?
“oceniacz złośliwości”
dla każdego
dostępny publicznie
nie wymaga bycia technicznym

Inny Antywirus

Prior art

Kilka antywirusów

Prior art

Kilka antywirusów

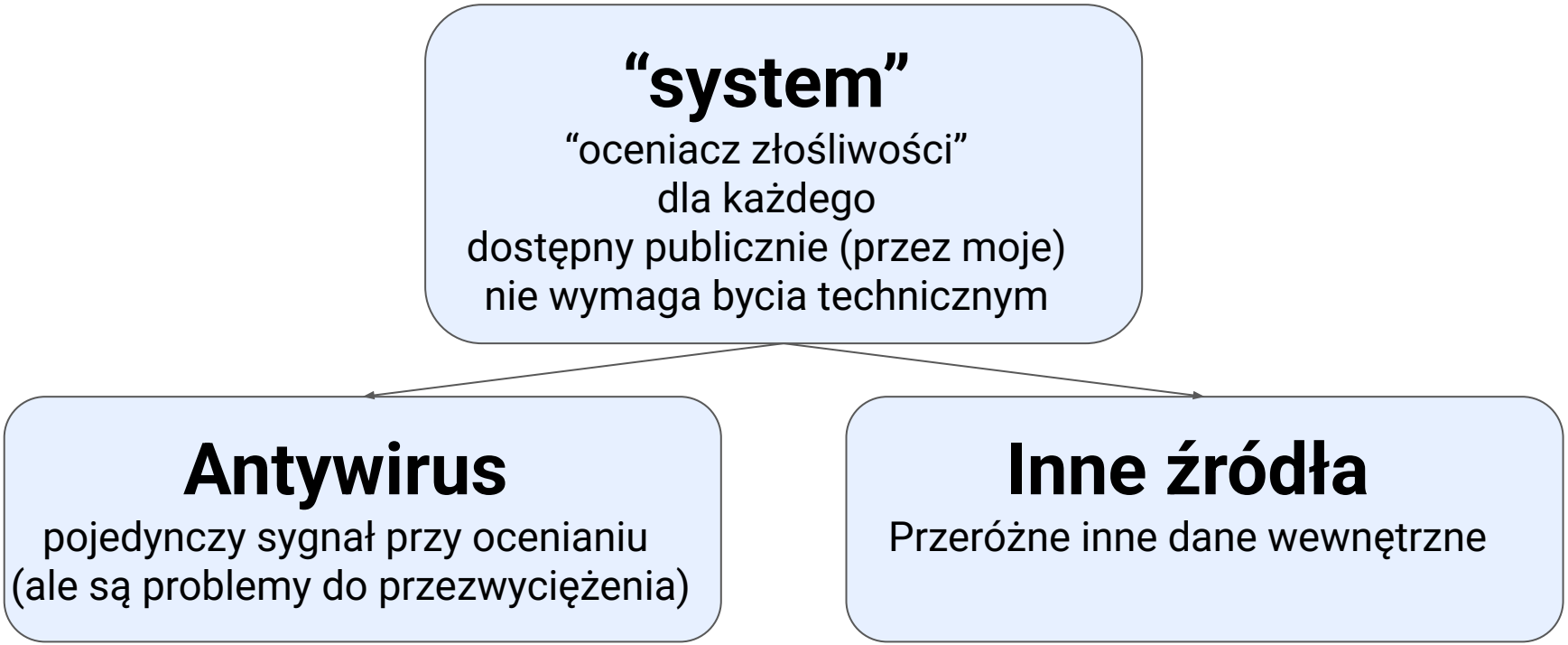
Prior art


Kilka antywirusów
VIRUSTOTAL
You have become the very thing you swore to destroy

Prior art


Kilka antywirusów
VIRUSTOTAL
2. Brak (prywatnego i skutecznego) gotowca
You have become the very thing you swore to destroy

Prior art


“system”
“oceniacz złośliwości”
dla każdego
dostępny publicznie (przez moje)
nie wymaga bycia technicznym
Antywirus
pojedynczy sygnał przy ocenianiu
(ale są problemy do przezwyciężenia)
Inne źródła
Przeróżne inne dane wewnętrzne

Źródła które już mamy

Źródła które już mamy

Źródła które już mamy

Źródła które już mamy

Źródła które już mamy

Źródła które już mamy

3. Istniejące dane które można integrować
3. Istniejące systemy które można zintegrować

Znamy najnowsze zagrożenia

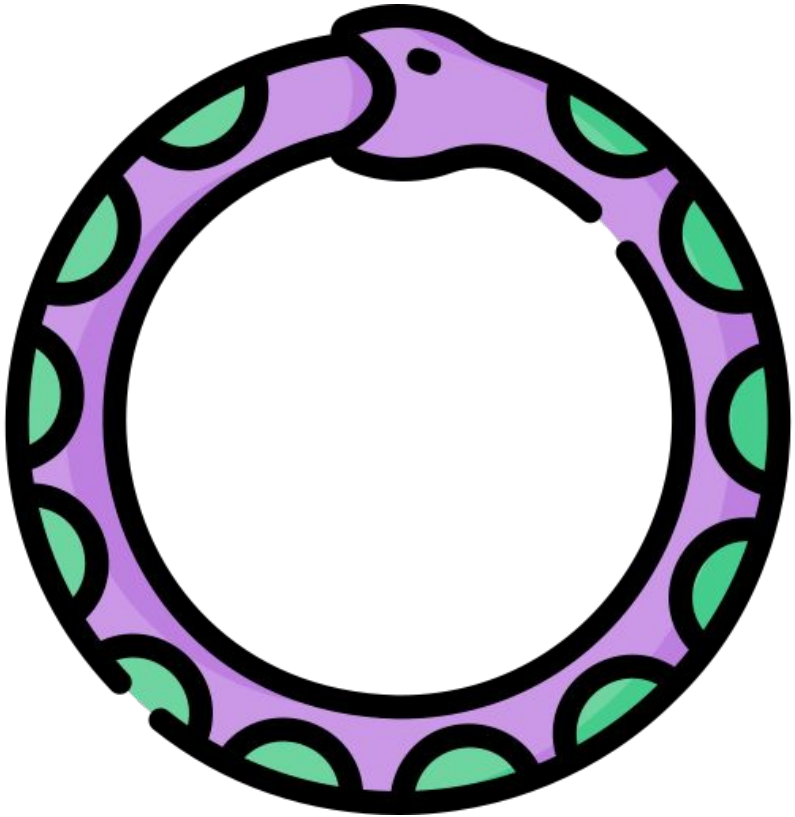
Name/SHA256/First seen	Size/Type/Tags
Kopia_patnosci.xls f602 Mon, 01 Dec 2025 02:20:40 GMT	**Size:** 1.52 MB **Type:** Composite Document File V2 Document, Can't read S... document:win32:xls ⊘ feed:pl-triage-new-and-malicious ⊘
Kopia_patnosci.xls af572 Sat, 29 Nov 2025 18:24:39 GMT	**Size:** 2.02 MB **Type:** ASCII text, with very long lines (65536), with no line t... document:win32:xls ⊘
Kopia_patnosci.xls b628(Wed, 26 Nov 2025 07:02:26 GMT	**Size:** 1.53 MB **Type:** Composite Document File V2 Document, Little Endian,... document:win32:xls ⊘ feed:malwarebazaar ⊘ feed:vx ⊘ ripped:remcos ⊘ yara:office_document_with_vba_project ⊘ yara:win_remcos ⊘

Znamy najnowsze zagrożenia

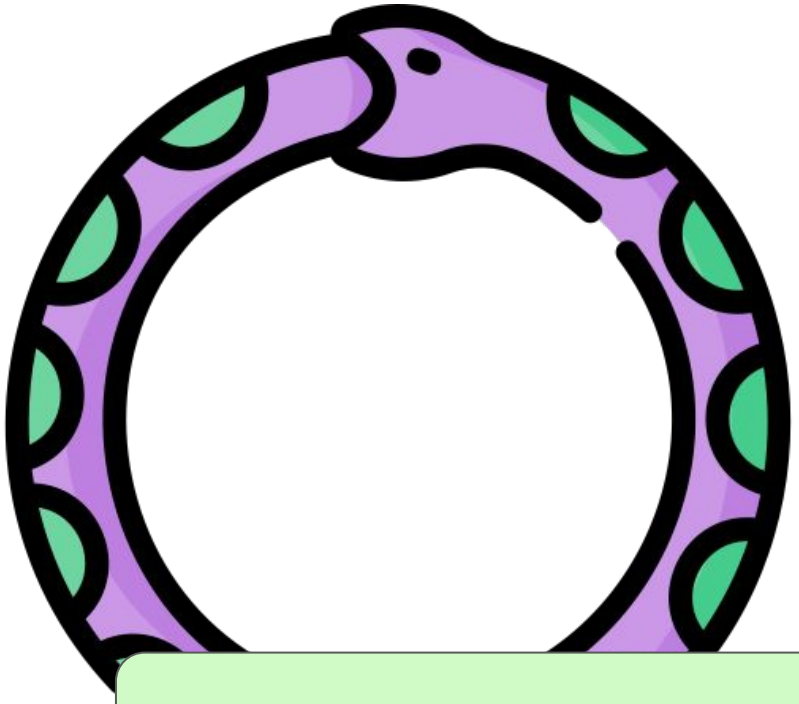
Name/SHA256/First seen	Size/Type/Tags
Kopia_patnosci.xls f602: Mon, 01 Dec 2025 02:20:40 GMT	**Size:** 1.52 MB **Type:** Composite Document File V2 Document, Can't read S... document:win32:xls ⃠ feed:pl-triage-new-and-malicious ⃠
Kopia_patnosci.xls af572 Sat, 29 Nov 2025 18:24:39 GMT	**Size:** 2.02 MB **Type:** ASCII text, with very long lines (65536), with no line t... document:win32:xls ⃠
Kopia_patnosci.xls b628(Wed, 26 Nov 2025 07:02:26 GMT	**Size:** 1.53 MB **Type:** Composite Document File V2 Document, Little Endian,... document:win32:xls ⃠ feed:malwarebazaar ⃠ feed:vx ⃠ ripped:remcos ⃠ yara:office_document_with_vba_project ⃠

4. Unikalna wiedza na temat polskich kampanii

Poznamy najnowsze zagrożenia



Poznamy najnowsze zagrożenia



5. Szansa nabycia jeszcze pełniejszej wiedzy

Co nam (i Wam) to da

1. Zapotrzebowanie constituency na skuteczne i prywatne rozwiązanie
2. Brak istniejącego, łatwo dostępnego produktu
3. Istnieją już systemy, które wystarczy zintegrować
4. Nasza unikalna wiedza na temat polskich zagrożeń
5. Źródło wiedzy na temat najnowszych kampanii

Co nam (i Wam) to da

1. Zapotrzebowanie constituency na skuteczne i prywatne rozwiązanie
2. Brak istniejącego, łatwo dostępnego produktu
3. Istnieją już systemy, które wystarczy zintegrować
4. Nasza unikalna wiedza na temat polskich zagrożeń
5. Źródło wiedzy na temat najnowszych kampanii

disclaimer: co będzie ostatecznie dostępne publicznie - do ustalenia

Podsumowując

Myśli końcowe

Podsumowując

“To co powinienem w takim razie zrobić?”

Podsumowując

“To co powinienem w takim razie zrobić?”

“Tak się składa, że w moje.cert.pl jest taka jedna funkcja…”

Podsumowując

“To co powinienem w takim razie zrobić?”

“Tak się składa, że w moje.cert.pl jest taka jedna funkcja…”

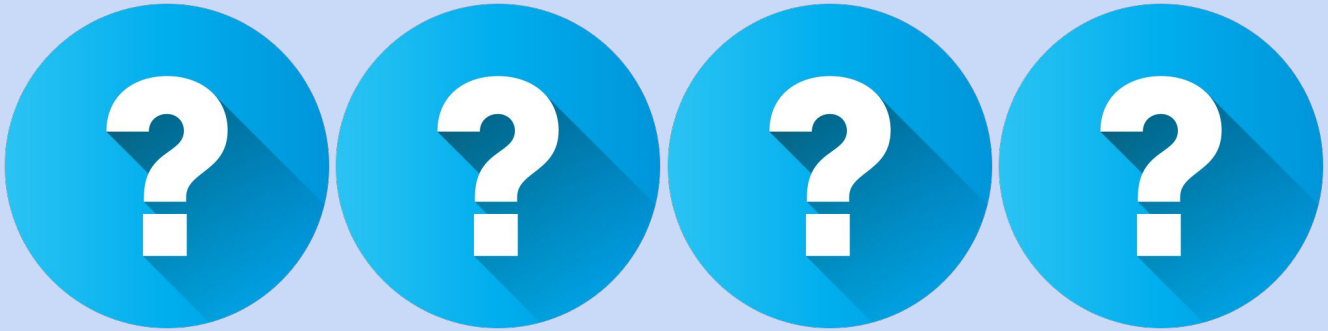
[wybierz opcję dialogową]

Dalej uważam, że to bez sensu.

OK, przekonałeś.

Q&A

jaroslaw.jedynak@cert.pl



Icons from flaticon.com by freepik, uniconlabs, roundicons, Ahsanu Nadia, Hight Quality Icons,