

Wykrywanie złośliwych plików?



Ale co w tym trudnego?

Tytułem wstępu

Reverse Engineering w

<CERT.PL>_

Tytułem wstępu

Reverse Engineering w

CERT.PL >_

Kiedyś też



Symantec

Google



Tytułem wstępu

Reverse Engineering w

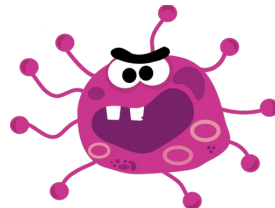
CERT.PL >_

Kiedyś też



Symantec

Google



Tytułem wstępu

Reverse Engineering w

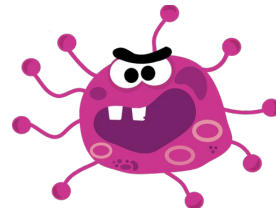
CERT.PL >_

Kiedyś też



Symantec

Google



?

Jaki w ogóle jest problem?

Tytułem wstępu

Reverse Engineering w

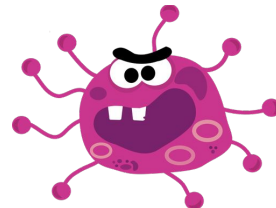
CERT.PL >_

Kiedyś też



Symantec

Google



?

Jaki w ogóle jest problem?

?

?

Jak go chcemy rozwiązać?

Tytułem wstępu

Reverse Engineering w

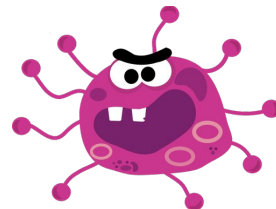
CERT.PL >_

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



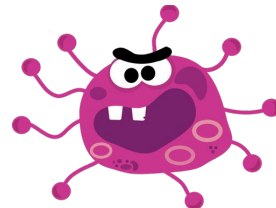
Jaki w ogóle jest problem?



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 pracy przyszła wiadomość z dziwnym



P 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 pracy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”



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

Problem





Search for IoCs, Threat Actors, or Malware

Smart search     



7
/ 62

Community Score -11

7/62 security vendors flagged this file as malicious

Follow

Reanalyze

Download

Similar

More

5aabf72f55a4af705981b581384c39aeba7b9c59d...

Size
163.96 KB

Last Analysis Date
3 hours ago



IMG-20251201-2025000173.tar

rar

attachment

DETECTION

DETAILS

RELATIONS

CONTENT

TELEMETRY

COMMUNITY 4

Security vendors' analysis on 2025-12-02T00:59:50 UTC

Popular threat label trojan.

Threat categories trojan

ESET-NOD32	JS/TrojanDropper.Agent.PVH Trojan	GData	Archive.Trojan.Agent.ANGL7C
Google	Detected	Google Safe Browsing	MALWARE
Gridinsoft (no cloud)	Trojan.U.AgentTesla.tr	Ikarus	Trojan-Downloader.JS.Agent
Varist	JS/Agent.DKF	Acronis (Static ML)	Undetected

ziwnym

!"

Problem



“Hmm, na mój e-mail pracy 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

- wykłady -

[LIVE ONLY] CZYM TWOJA FIRMA
DZIELI SIĘ ZE MNĄ NA VIRUS
TOTALU?

Dec 5 / 12:00 - 12:45

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 pracy przyszła wiadomość z dziwnym załącznikiem. Ciekawe czy mogę go otworzyć.”



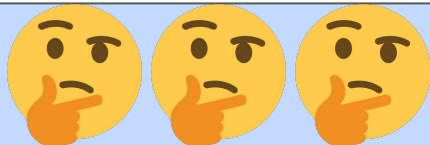
“Daj mi swój plik. Przeanalizuję go dla Ciebie za darmo!”



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



“To co powinienem w takim razie zrobić?”



Problem (z rekomendacją)



“Nie otwieraj podejrzanych
załączników!”

Problem (z rekomendacją)



~~"Nie otwieraj podejrzanych
załączników!"~~

Problem (z rekomendacją)



~~“Nie otwieraj podejrzanych załączników!”~~



“Zapytaj nadawcę innym kanałem.”

Problem (z rekomendacją)



~~"Nie otwieraj podejrzanych załączników!"~~



"Zgłoś incydent do CERTu?"



"Zapytaj nadawcę innym kanałem."

Problem (z rekomendacją)



~~“Nie otwieraj podejrzanych załączników!”~~



“Zgłoś incydent do CERTu?”



“Zapytaj nadawcę innym kanałem.”



“Zgłoś do swojego działu bezpieczeństwa?”

Problem (z rekomendacją)



~~“Nie otwieraj podejrzanych załączników!”~~



“Zgłoś incydent do CERTu?”



“Wrzuć do firmowego sandboxa ale nie VirusTotala proszę!”



“Zapytaj nadawcę innym kanałem.”



“Zgłoś do swojego działu bezpieczeństwa?”

Problem (z rekomendacją)



~~“Nie otwieraj podejrzanych załączników!”~~



“Zgłoś incydent do CERTu?”



“Wrzuć do firmowego sandboxa ale nie VirusTotala proszę!”



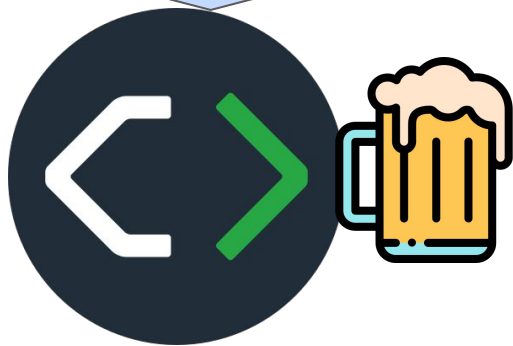
“Zapytaj nadawcę innym kanałem.”



“Zgłoś do swojego działu bezpieczeństwa?”

Problem (z rekomendacją)

W sumie czemu tego nie zrobić samemu?

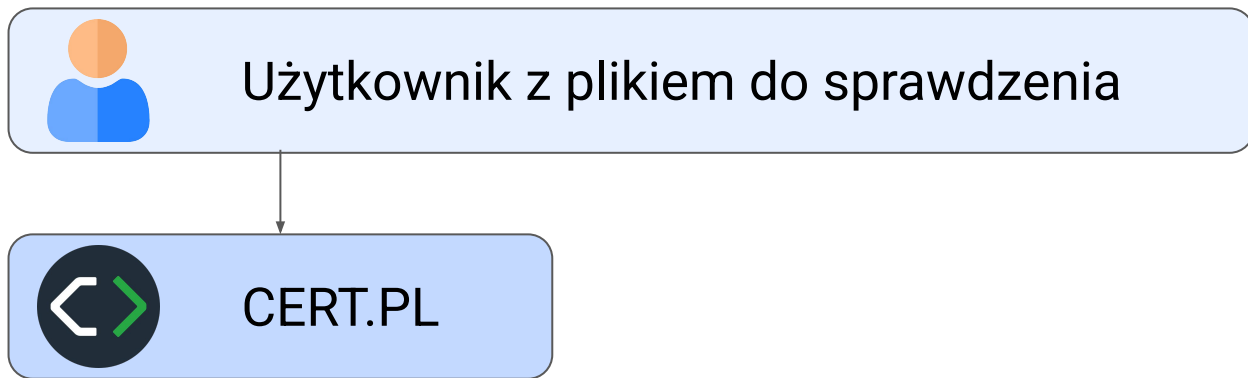


Pomysł

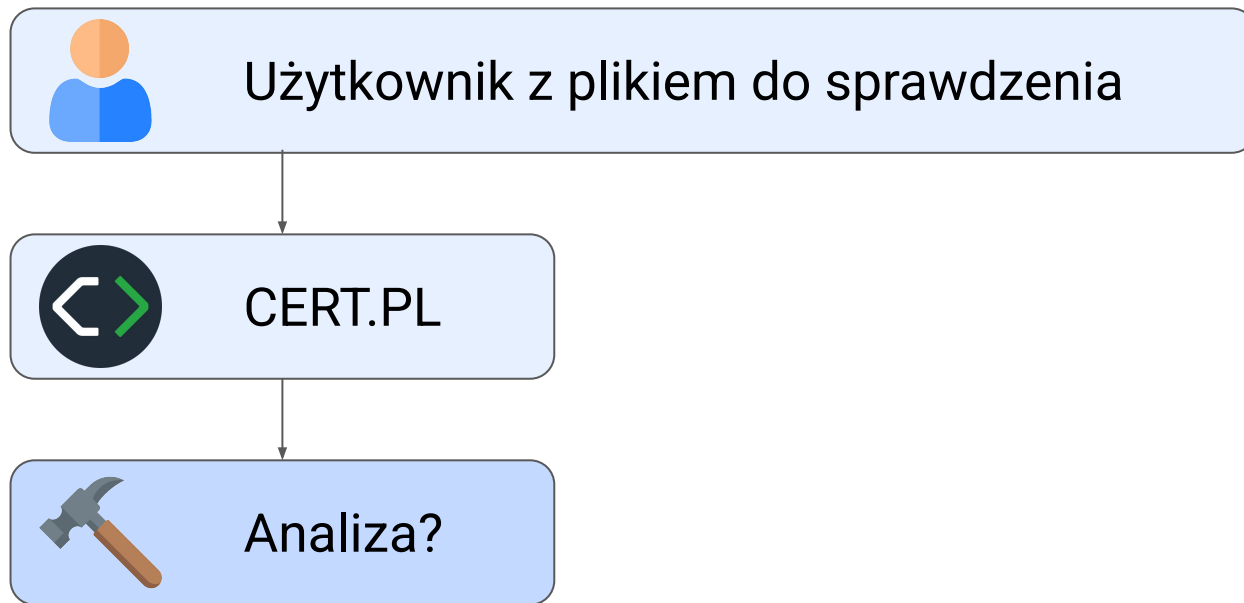


Użytkownik z plikiem do sprawdzenia

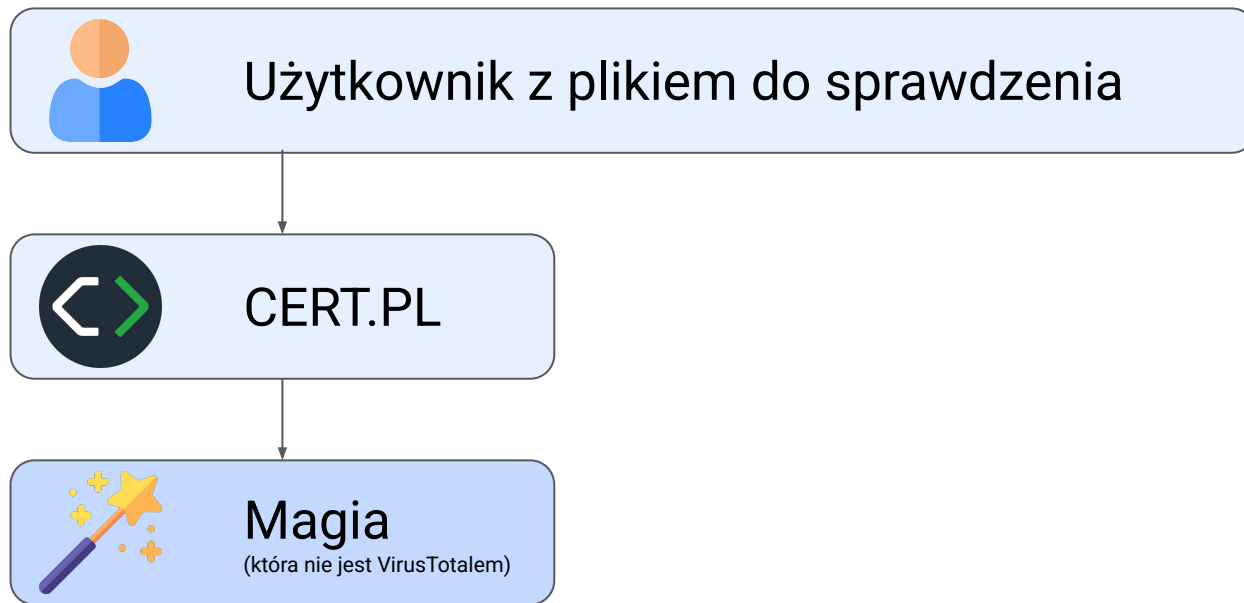
Pomysł



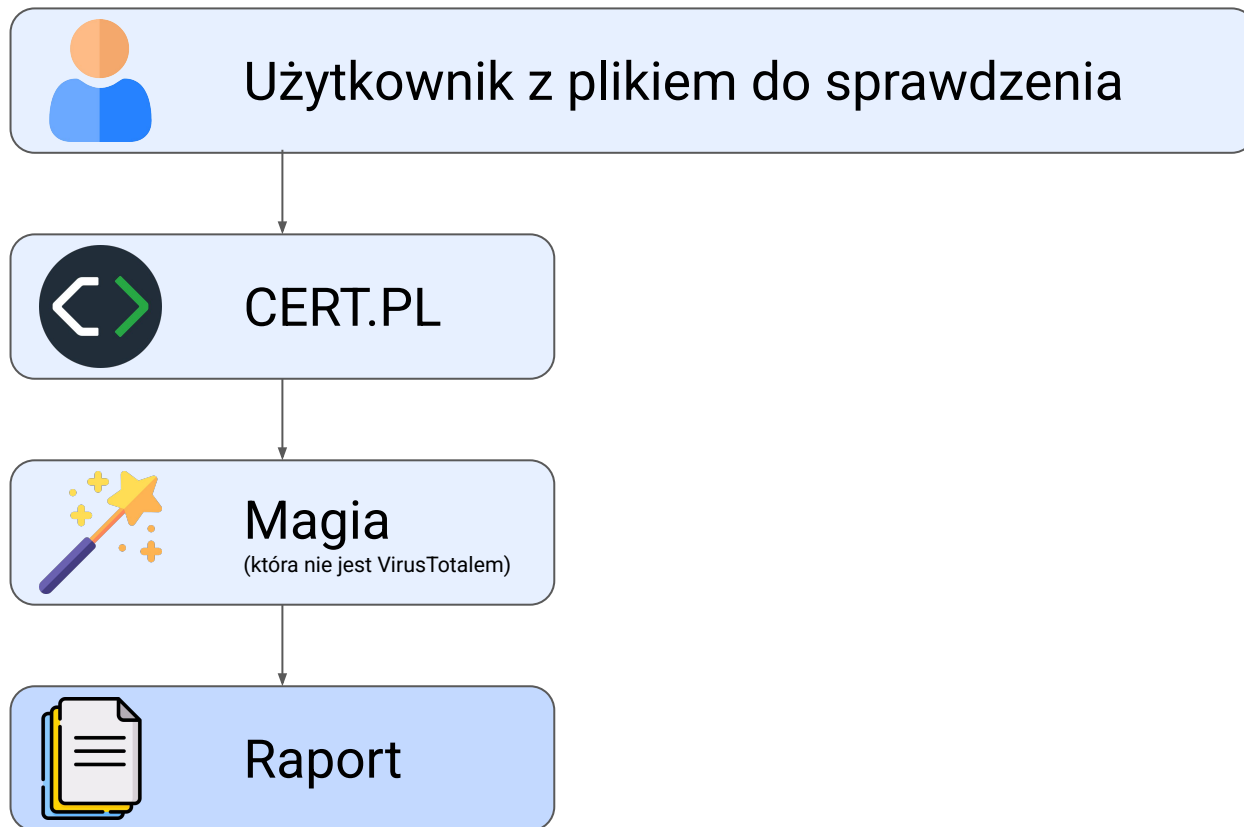
Pomysł



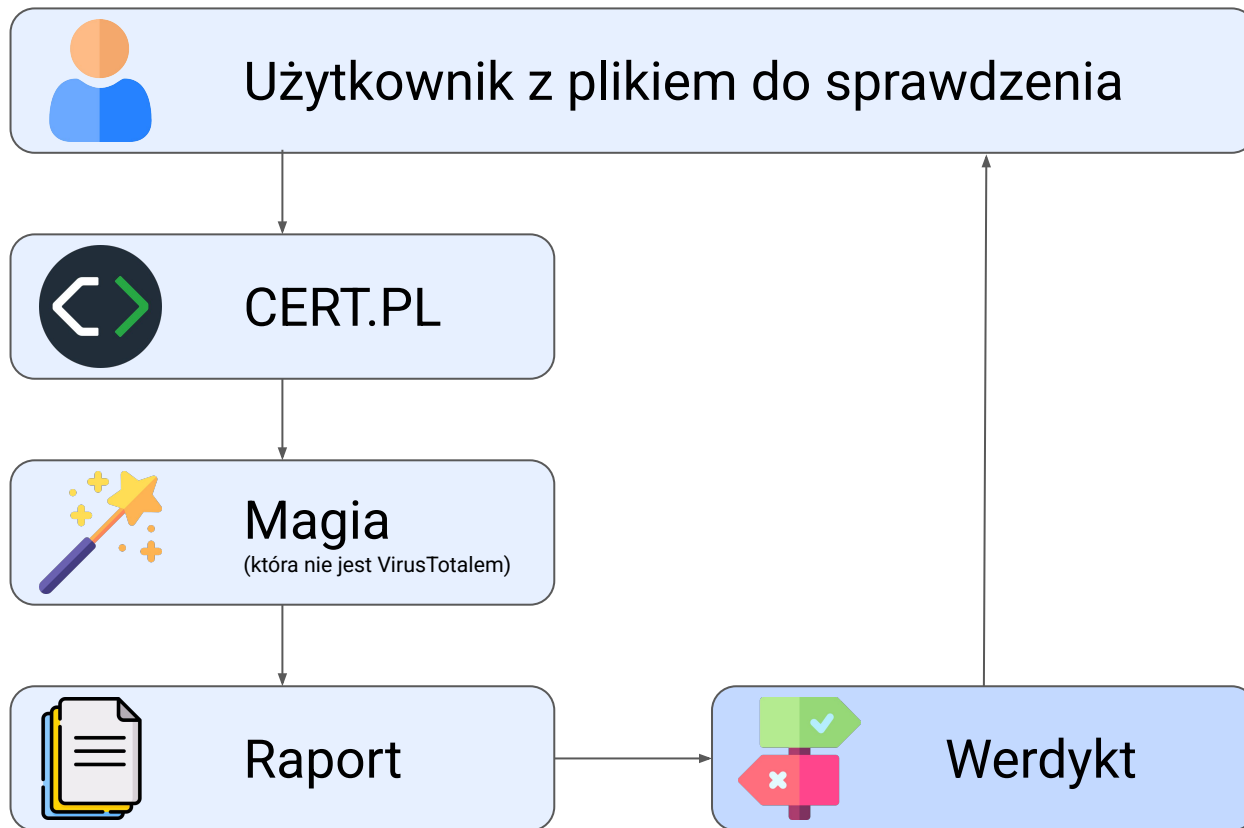
Pomysł



Pomysł



Pomysł



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



kasja.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



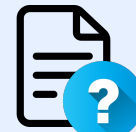
Kopia_patnosci.xls



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”

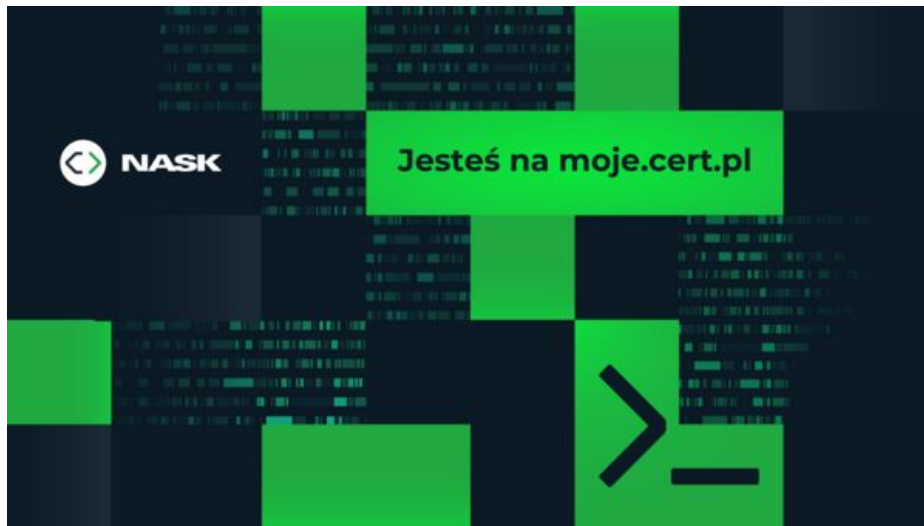
Publiczny interfejs

moje.cert.pl

Publiczny interfejs

moje.cert.pl

usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przístupne dla osób technicznych



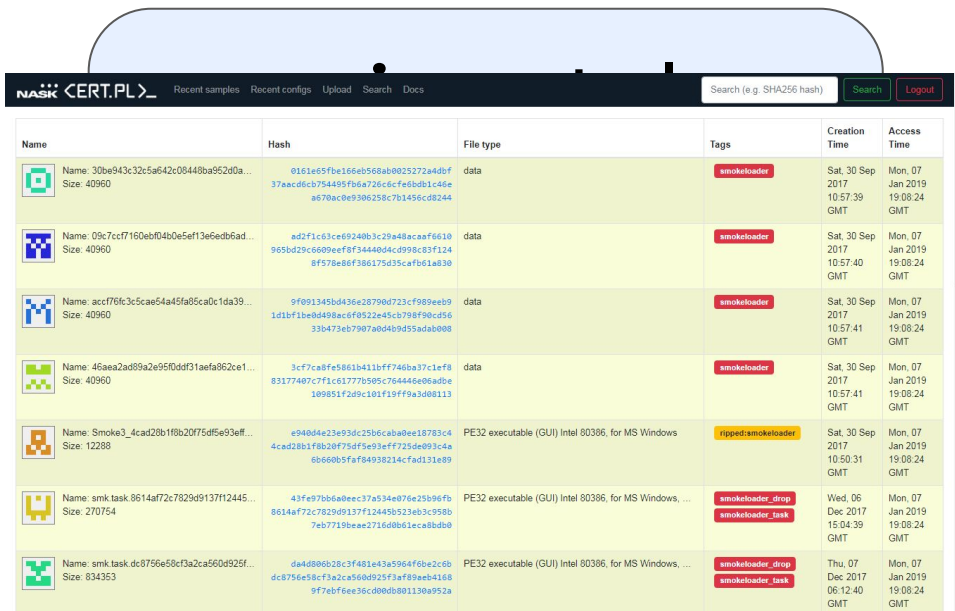
Publiczny interfejs

moje.cert.pl

usługi bezpieczeństwa
dla administratorów
otwarta rejestracja
przystępne dla osób technicznych

mwdb.cert.pl

Publiczny interfejs



The screenshot shows the mwdb.cert.pl public interface. At the top, there's a navigation bar with links: Recent samples, Recent configs, Upload, Search, Docs. A search bar is present with the placeholder text "Search (e.g. SHA256 hash)". Below the navigation bar, there's a table listing malware samples. The table has columns: Name, Hash, File type, Tags, Creation Time, and Access Time. The first five samples are of type 'data' and are tagged 'smokeloader'. The next sample is a 'PE32 executable (GUI) Intel 80386, for MS Windows' tagged 'ripped:smokeloader'. The last two samples are also 'PE32 executable (GUI) Intel 80386, for MS Windows' and are tagged 'smokeloader_drop' and 'smokeloader_task'.

Name	Hash	File type	Tags	Creation Time	Access Time
 Name: 30be943c32e5a642c08440ba962da... Size: 40960	0161e5fba185eb980ab0025272a4dbf 37aac6fc6754495f6a7264c6cf6bd1c46e a670ac0e9306255c761456cd8244	data	smokeloader	Sat, 30 Sep 2017 10:57:39 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: 09c7cc7f160eb04b0e5ef13e6edb6ad... Size: 40960	ad2f1c63ce9240b3c29e48aca76610 965bd29c609ee0f93444004c0998c83f124 8f57ba06f386179d35cafd61a830	data	smokeloader	Sat, 30 Sep 2017 10:57:40 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: accf76fc3c5cae54a45fa05ca0c1da39... Size: 40960	9f091345bd43ee28790d723cf989eeb9 1d1bf1be0d49aac6f0522e45cb798f90cd56 33b473eb7907a0409655ada0080	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: 46aea2ad89a2e9f0dd31aefa962ce1... Size: 40960	3cf7ca8fe5861b411bf7f46ba37c1ef8 83177407c7f1c6177b505c764446e0ead0e 189851f2d9c101f19ff9a3d80113	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: Smoke3_4cad28b1f8b20f75df5e93ef... Size: 12288	e940d4e23e93dc25b6cab0ee18783c4 4cad28b1f8b20f75df5e93ef7725de093c4a 6b660b5fa84930214cfad13189	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.8614af72c7829d913712445... Size: 270754	43fe97b6da0ec37a534e076e25b96fb 8614af72c7829d913712445b523eb3c98b 7eb7719beae2716d0b61eca8bd0	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	da4d086b28c3f481e43a5964f6be2c6b dc8756e58cf3a2ca560d925f3af89aee4168 9f7ebf6ee36cd0bd0801130a952a	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

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

Publiczny interfejs

NASK CERT.PL >_

[Recent samples](#)

[Recent configs](#)

[Upload](#)

[Search](#)

[Docs](#)

Search (e.g. SHA256 hash)

[Search](#)

[Logout](#)

Name	Hash	File type	Tags	Creation Time	Access Time
 Name: 30be943c32c5a642c08448ba952d0a... Size: 40960	0161e65f6e166eb568ab0025272a4dbf 37aacd6cb754495fb6a726c6cf6b6b1c46e a670ac0e9306258c7b1456cd8244	data	smokeloader	Sat, 30 Sep 2017 10:57:39 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: 09c7ccf7160ebf04b0e5ef13e6edb6ad... Size: 40960	ad2f1c63ce69240b3c29a48acaaf6610 965bd29c6609eef8f34440d4cd998c83f124 8f578e86f386175d35caf6b1a830	data	smokeloader	Sat, 30 Sep 2017 10:57:40 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: accf76fc3c5cae54a45fa85ca0c1da39... Size: 40960	9f091345bd436e28790d723cf989eeb9 1d1bf1be0d498ac6f0522e45cb798f90cd56 33b473eb7907a0d4b9d55adab008	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: 46aea2ad89a2e95f0ddf31aefa862ce1... Size: 40960	3cf7ca8fe5861b411bff746ba37c1ef8 83177407c7f1c61777b505c764446e06adbe 109851f2d9c101f19ff9a3d08113	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
 Name: Smoke3_4cad28b1f8b20f75df5e93eff... Size: 12288	e940d4e23e93dc25b6caba0ee18783c4 4cad28b1f8b20f75df5e93eff725de093c4a 6b660b5faf84938214cfad131e89	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	43fe97bb6a0eec37a534e076e25b96fb 8614af72c7829d9137f12445b523eb3c958b 7eb7719beae2716d0b61eca8bdb0	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	da4d806b28c3f481e43a5964f6be2c6b dc8756e58cf3a2ca560d925f3af89aeb4168 9f7ebf6ee36cd00db801130a952a	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

CERT.PL

Samples

Configs

Blobs

Upload

Search

Settings

Statistics

About

msm

Logout

File details



Details



Relations



Preview

Static config

asyncrat



Apivectors

Actions

File name 2025-12-02_9ab5f55aae63588ba9fb40c7bd1f29d6_amadey_asyncrat_elex_glassworm_smoke-loader

Variant file names

File size 6.26 MB

File type PE32 executable for MS Windows 5.01 (GUI), Intel i386, 5 sections

md5 9ab5f55aae63588ba9fb40c7bd1f29d6

sha1 584d3944ed97d6c301b9fd8f657c6bcbbe89ae70

sha256 3d66138163912234690370a903f697d1aec3f66992666463ea038c795012cf99

sha512 a1552d539ffcc201b59c2538caada9bd9e9aaa2731e6bd8f3eb744e5d0d76311c580e1dd4fa37d51856f9ee9d9e4afd05e21351672b40c4adf0e6a0c5c336af3

crc32 4c1fb68c

ssdeep 98304:CErLCY0C1cTgtU4+UXN5G52ghi/J6xW21yuzvS17umbrSANjM0yyVlpJ43v:CErUy7qMe4+aNoGM3subfCmbr1n40DV

Upload time Tue, 02 Dec 2025 05:06:45 GMT

Tags

asyncrat X

feed:vx X

ripped:asyncrat X

runnable:win32:exe X

yara:indicator_suspicious_exe_cc_regex X

yara:indicator_suspicious_exe_discord_regex X

yara:indicator_suspicious_exe_references_confidential_data_store X

yara:indicator_suspicious_exe_references_vpn X

yara:indicator_suspicious_exe_sandboxhookingdll X

yara:indicator_suspicious_exe_telegramchatbot X

yara:indicator_suspicious_exe_vaultschemaguid X

yara:indicator_suspicious_exe_wirelessnetrecon X

yara:malware_win_celestybinerloader X

yara:malware_win_multi_family_infostealer X

yara:malware_win_worldwind X

yara:sandboxdetect_misc X

yara:susp_net_msil_suspicious_use_strreverse X

yara:win_asyncrat X

Add tag

Add

Related configs: 1

+ Add

child

bfaa426f710aa9275a9702e23e29057c2242a14895923f298d99f006e4f01975

Karton analyses

+ Reanalyze

przys

edzy

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

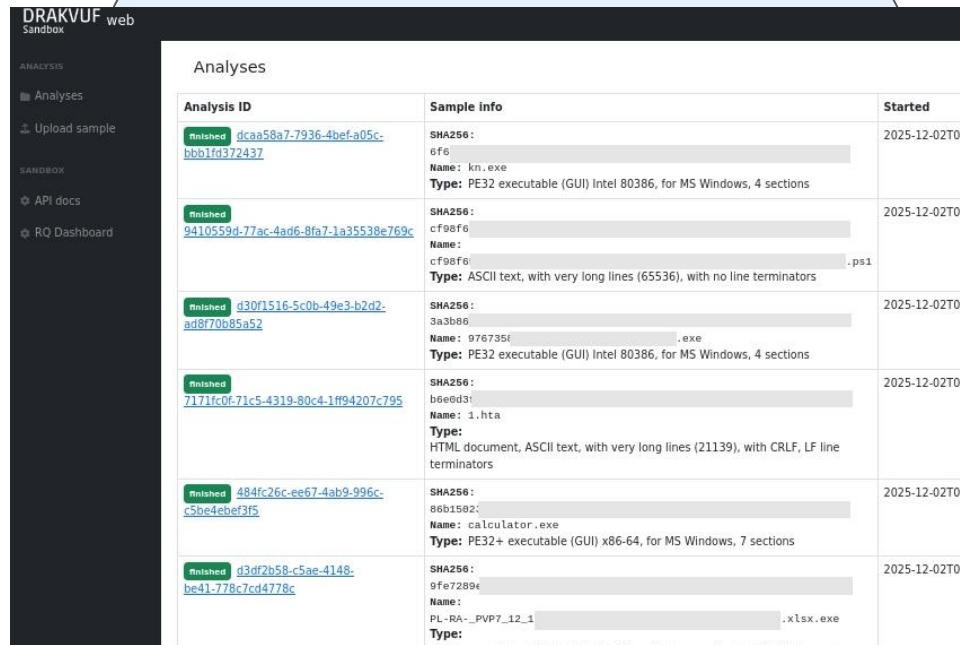
Publiczny interfejs

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



The screenshot shows the DRAKVUF web interface. On the left is a dark sidebar with navigation links: 'Analyses', 'Upload sample', 'API docs', and 'RQ Dashboard'. The main area is titled 'Analyses' and contains a table with analysis results.

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 Type: ASCII text, with very long lines (65536), with no line terminators	2025-12-02T0
finished d30f1516-5c0b-49e3-b2d2-ad8f70b85a52	SHA256: 3a3bb6 Name: 076735f.exe Type: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections	2025-12-02T0
finished 7171fc0f-71c5-4319-80c4-1ff94207c795	SHA256: b6e0d3f 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: 9fe7289e Name: PL-RA--PVP7_12_1.xlsx.exe Type:	2025-12-02T0

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: 976735f.exe Type: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections	2025-12-02T0
Finished 7171fc0f-71c5-4319-80c4-1ff94207c795	SHA256: b6e0d3f 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: 86b1502f Name: calculator.exe Type: PE32+ executable (GUI) x86-64, for MS Windows, 7 sections	2025-12-02T0
Finished d3df2b58-c5ae-4148-be41-778c7cd4778c	SHA256: 9fe7289e Name: PL-RA-_PVP7_12_1.xlsx.exe Type:	2025-12-02T0

Publiczny interfejs

Analysis report

- + System (4)
 - csrss.exe (464)
- + wininit.exe (540)
 - csrss.exe (548)
- winlogon.exe (636)
 - fontdrvhost.exe (784)
 - dwm.exe (8)
 - userinit.exe (4468)
 - explorer.exe (4488)
 - chrome.exe (3280)
 - rundll32.exe (3584)
 - taskmgr.exe (3756)
 - taskmgr.exe (4336)

File name	wtsapi32.dll
SHA256	a3b7ad3ac10b437dbe004aa6ec90b480a14304f2d5c59
Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows,
Start command	rundll32.exe wtsapi32.dll,QueryActiveSession
Analysis time	600 seconds
Job started at	2025-09-26T15:08:12.328900+00:00
Execution started at	2025-09-26T15:08:21.703890+00:00
Job finished at	2025-09-26T15:19:28.072045+00:00
Plugins	apimon filetracer memdump procmon socketmon tls

Download PCAP

TLS keys

Memory dumps

Publiczny interfejs

Summary report

General logs

Process info

Screenshots

Analysis files

— Process creation Success

Process name: rundll32.exe `rundll32.exe:3584`

Arguments: wtsapi32.dll,QueryActiveSession

Exited at: 1758899303.599354

Exit code: STATUS_SUCCESS (0x0)

Terminated by: (self)

— Domain queries 2

- settings-win.data.microsoft.com `RUXIMICS.exe:2584`
- dns.msftncsi.com `svchost.exe:1712`

— HTTP requests 1

- GET settings/v3.0/WSD/RUXIM?os=Windows&osVer=10.0.19045.5854.amd64fre.vb_release.191206-1406&sku=48&deviceCl:
Host: settings-win.data.microsoft.com:443
Process: `RUXIMICS.exe:2584`

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

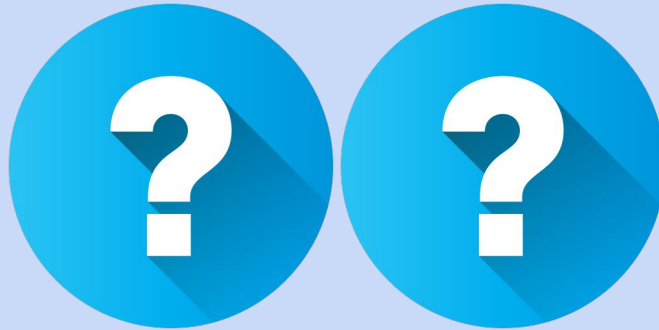
sandbox malware
dla analityków malware
kod na GitHubie
bardzo niszowa wiedza

“system”

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

Część 2

Jak go chcemy rozwiązać?

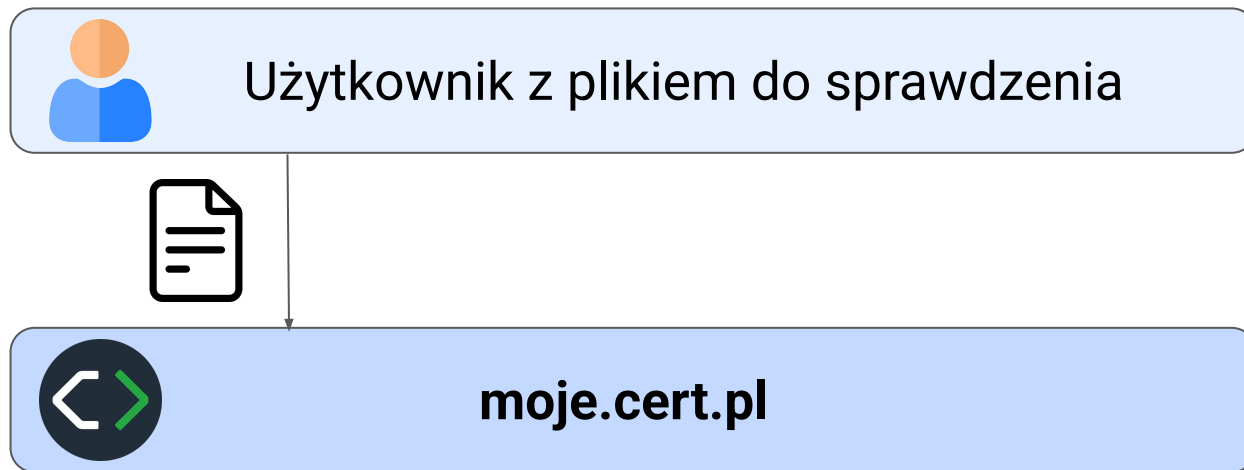


Po pierwsze: API

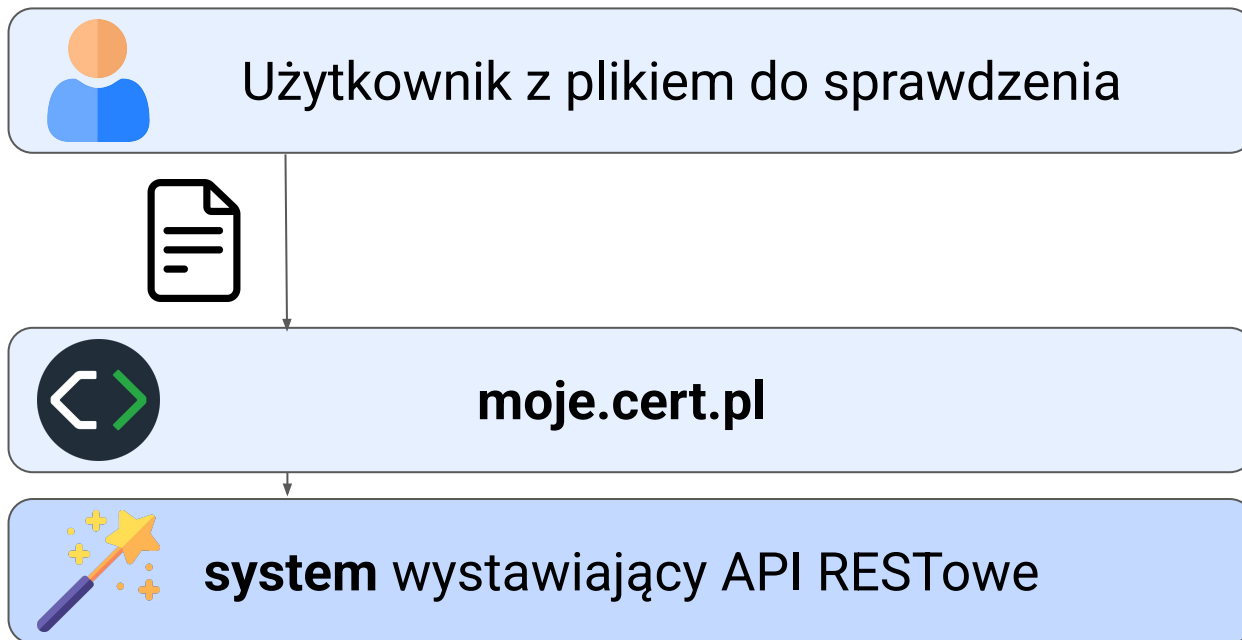


Użytkownik z plikiem do sprawdzenia

Po pierwsze: API



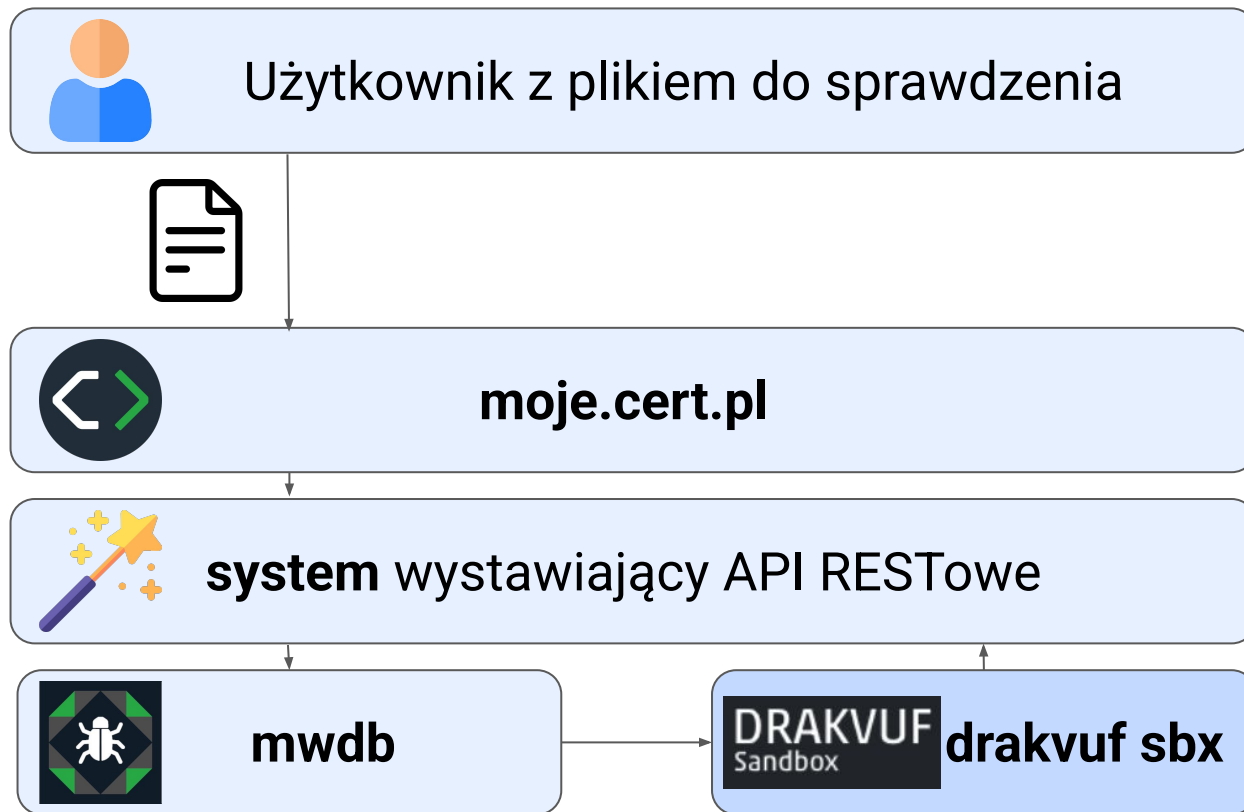
Po pierwsze: API



Po pierwsze: API



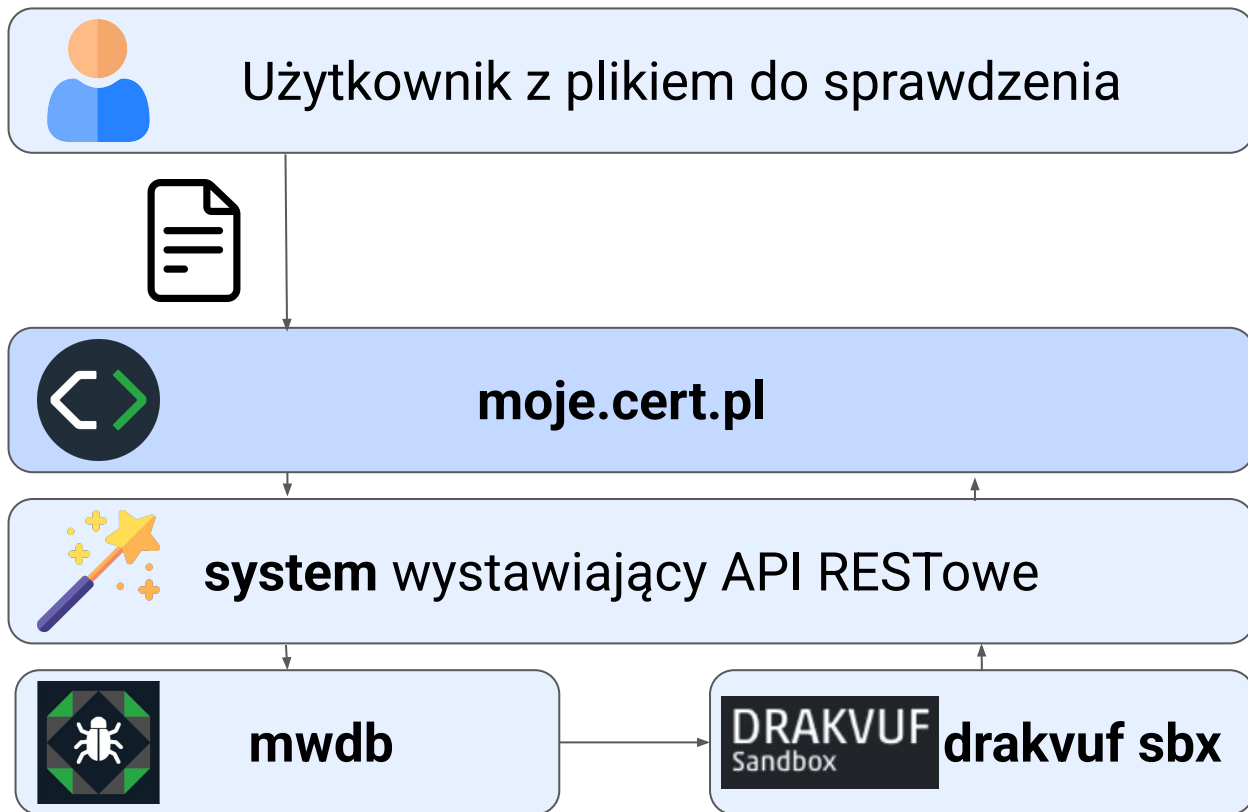
Po pierwsze: API



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 X

runnable:win32:exe X

yara:win_agent_tesla X

Family	xworm
Config type	static
+ ChatID	7588932713
+ Group	XWorm V6.5 by c31estial.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.



Name: PO_ASQT2510153810.exe
SHA256: ff30d24b652e2bd46709c8b3a
MD5: abb587c7cab32c2a9e23903c



Name: PO_ASQT2510153810.rar
SHA256: e1e1f7f3beb9c4a9340c8c99
MD5: 6f1eeee67dda95d7a3dacc14



Name: PO_ASQT2510153810.com
SHA256: ae91525ecd727e79110dcc98
MD5: 6048cd4c221567cfc7890d71



Name: PO_ASQT2510153810.arj
SHA256: f415ccb4786c84ac5f318d2f
MD5: 0cf8cf09f5cd318b62fd6b2d



Name: PO_n.144_-_0074.vbs
SHA256: 4c5ca4ce2fb9e3a9225555bcl
MD5: 05f100443aa2b04e0b0654db

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



es

,
ngu,
are.

Silnik analityczny

mwdb

wszy
powiąz
naz

a



es

,
ngu,
are.

Silnik analityczny

mwdb

wszy
powiąz
naz

a



es

,
ngu,
are.

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

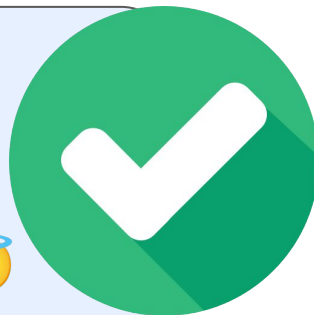


Podejrzana nazwa: 15% 😈

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

Software Execution x								
selection controls layer controls technique controls								
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (6/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Exploitation for Client Execution	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Shared Modules	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Scheduled Task/Job (3/6)	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture
Phishing (2/3)	Software Deployment Tools	Boot or Logon Autostart Execution (8/12)	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Time Discovery	Internal Spearphishing	Automated Collection
Supply Chain Compromise (1/3)	Inter-Process Communication (2/2)	Compromise Client Software Binary	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Network Connections Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media
Trusted Relationship	System Services (2/2)	External Remote Services	Abuse Elevation Control Mechanism (4/4)	BITS Jobs	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser
	User Execution (2/2)	Scheduled Task/Job (3/6)	Boot or Logon Initialization Scripts (3/5)	Hijack Execution Flow (7/11)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive
		Boot or Logon Initialization Scripts (3/5)	Create or Modify System Process (4/4)	Masquerading (5/6)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Cloud Storage Object
		Create Account (2/3)	Event Triggered Execution (10/15)	Traffic Signaling (0/1)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Configuration Repository (0/2)
		Event Triggered Execution (10/15)		Indirect Command Execution	Steal Application Access Token	Network Service Scanning		Data from Information Repositories (1/2)
		Implant Container Image		Group Policy Modification	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Data Staged (1/2)
				Rogue Domain Controller		Software Discovery (1/1)		Email Collection (2/3)
				XSL Script Processing		Network Sniffing		Input Capture (3/4)
				Abuse Elevation Control Mechanism (4/4)				
				Direct Volume Access				

T1059.003
(Windows Command Shell)

T1555.003
(Credentials from Web Browsers)

Indykatory



[Website](#) | [Download](#) | [Web Interface](#)

python 3 release v9.3.1 rules 1017 CI passing downloads 460k license Apache-2.0

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

```
{
  "name": "enumerate processes",
  "att&ck": [
    "Discovery::Process Discovery [T1057]",
    "Discovery::Software Discovery [T1518]"
  ],
  "occurrences": [
    {
      "ppid": 1356,
      "pid": 576
    }
  ]
}
```

[2024 Program](#) | [The Honeynet Project](#)

Contributor

Yacine Elhamer

[View
Code](#)

Extending the DRAKVUF Sandbox analytic pipeline

Mentors

Jarosław Jedynak

Organization

The Honeynet Project

Część 3

Co nam (i Wam) to da?



Żywotne potrzeby społeczeństwa



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

Żywotne potrzeby społeczeństwa



“Hmm, na mój e-mail pracy 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

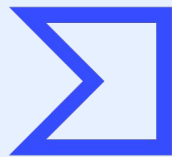
**Inny
Antywirus**

Prior art

Kilka antywirusów

Prior art

Kilka antywirusów

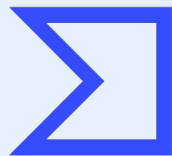


VIRUSTOTAL

Prior art



Kilka antywirusów

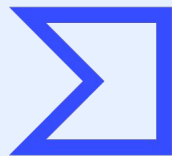


VIRUSTOTAL

You have become the very thing you swore to destroy

Prior art

Kilka antywirusów

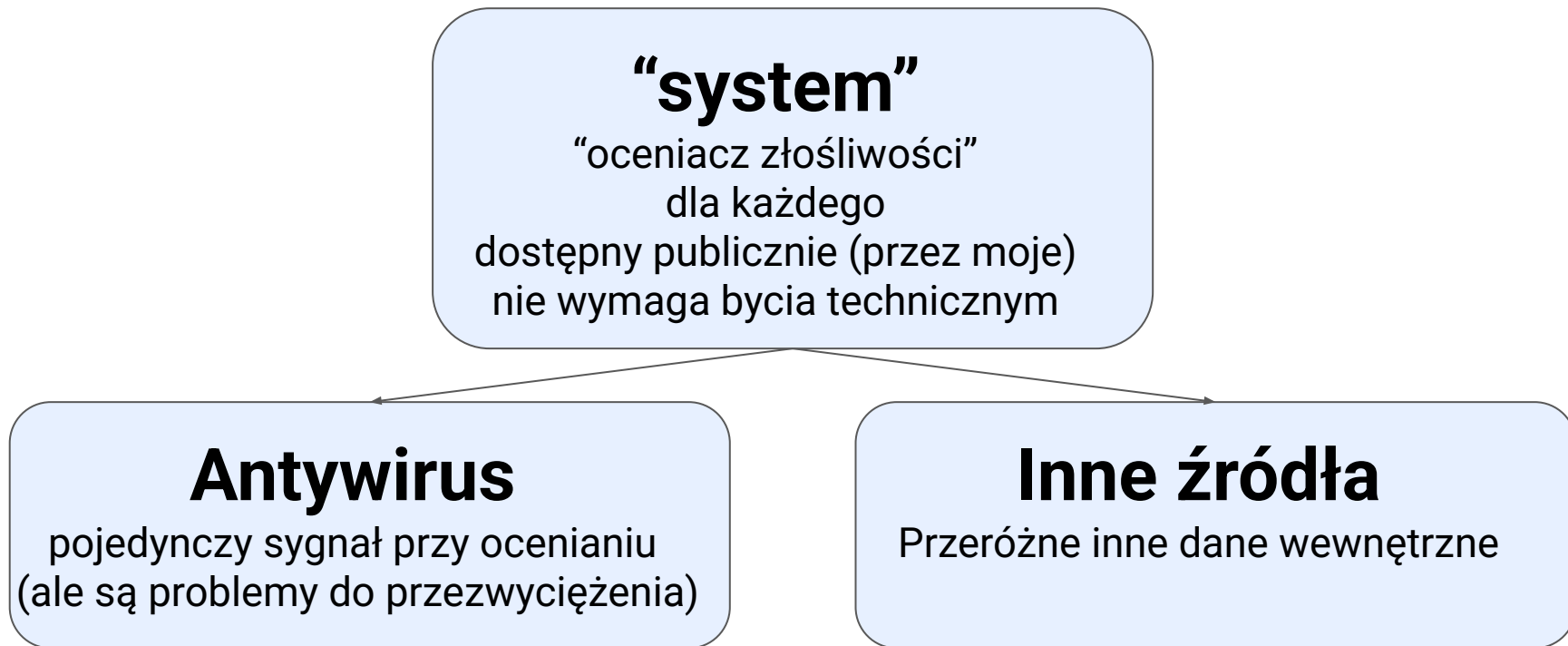


VIRUSTOTAL

2. Brak (prywatnego i skutecznego) gotowca

You have become the very thing you swore to destroy

Prior art



Źródła które juŹ mamy

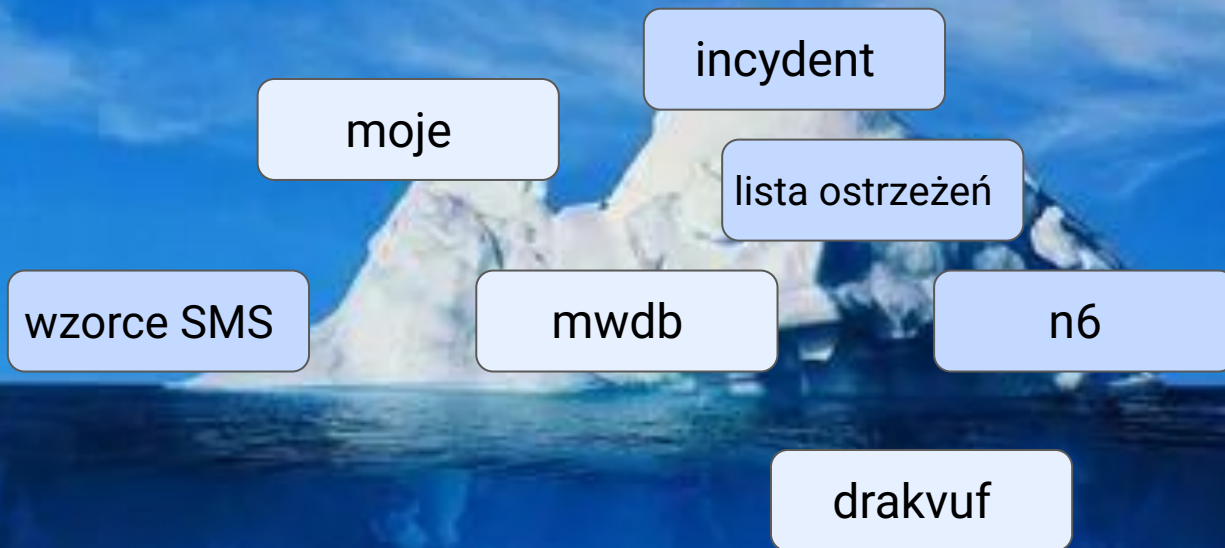
An iceberg floating in the ocean under a blue sky. The visible tip of the iceberg is labeled with 'moje' and 'mwdb'. The much larger, submerged part of the iceberg is labeled with 'drakvuf'.

moje

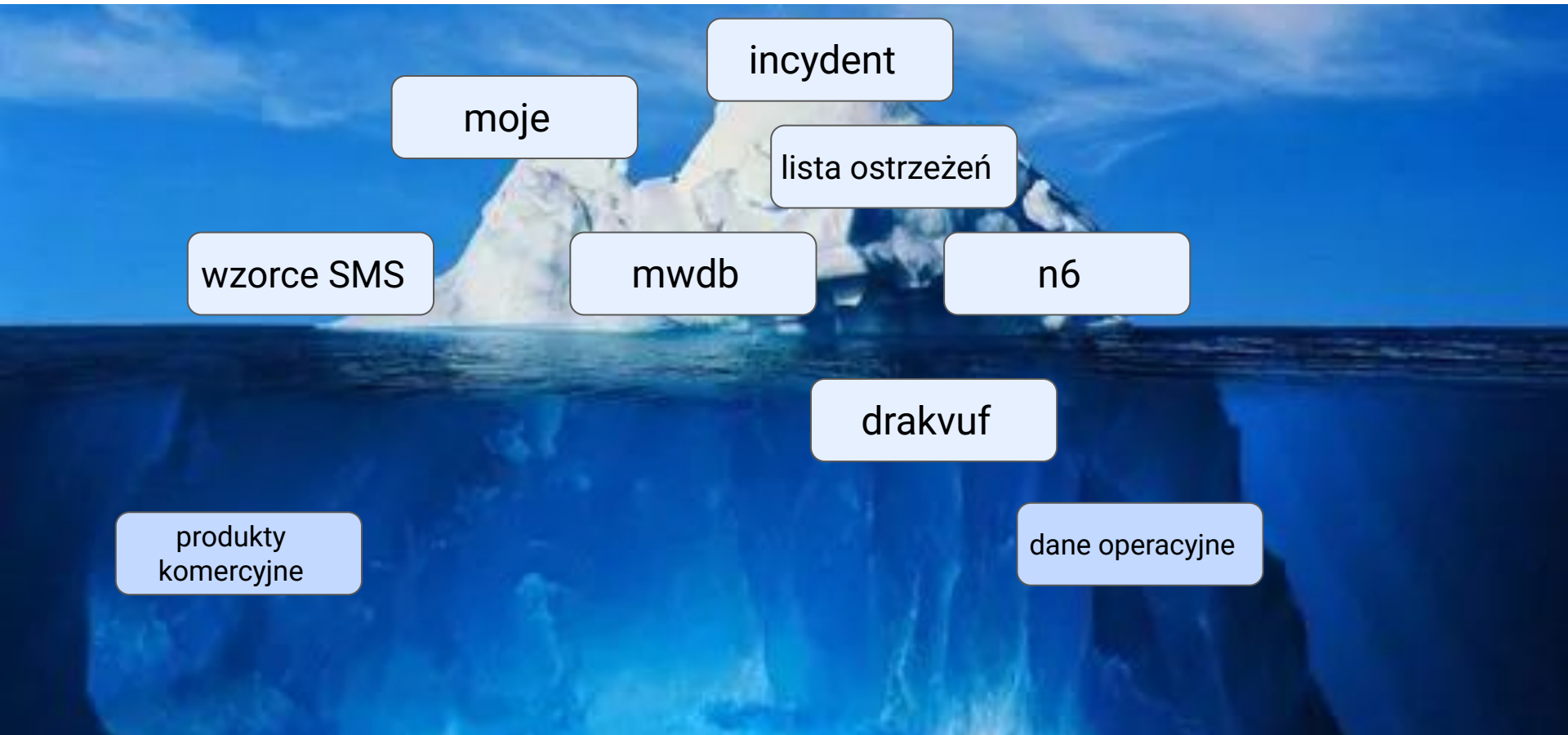
mwdb

drakvuf

Źródła które już mamy



Źródła które już mamy



incydent

moje

lista ostrzeżeń

wzorce SMS

mwdb

n6

drakvuf

produkty
komercyjne

dane operacyjne

Źródła które już mamy



Źródła które już mamy

wzorce SMS

moje

incydent

lista ostrzeżeń

mwdb

n6

drakvuf

produkty
komercyjne

karton

dane operacyjne

3. Istniejące dane które można integrować

Źródła które już mamy



Znamy najnowsze zagrożenia

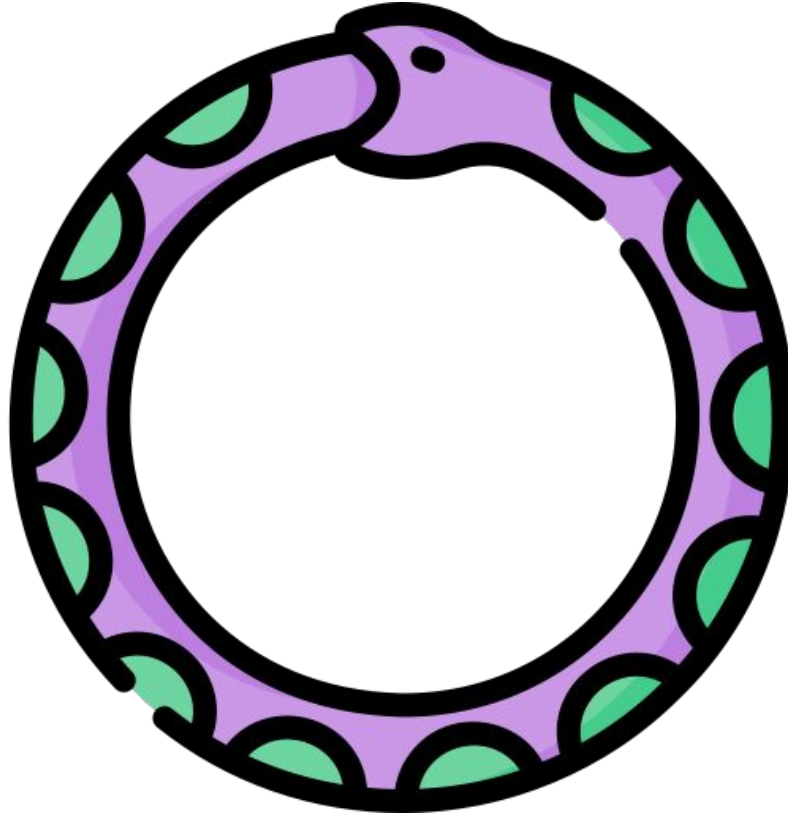
Name/SHA256/First seen	Size/Type/Tags
Kopia_patnosci.xls f602: Mon, 01 Dec 2025 02:20:40 GMT	Size: 1.52 MB Type: Composite Document File V2 Document, Can't read S... document:win32:xls feed:pl-triage-new-and-malicious
Kopia_patnosci.xls af572 Sat, 29 Nov 2025 18:24:39 GMT	Size: 2.02 MB Type: ASCII text, with very long lines (65536), with no line t... document:win32:xls
Kopia_patnosci.xls b6286 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:wln_remcos

Znamy najnowsze zagrożenia

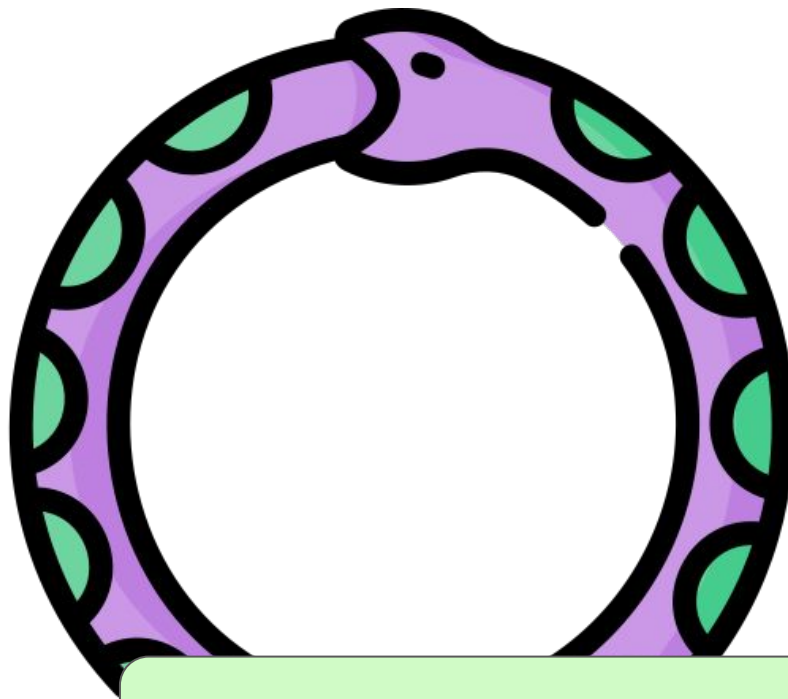
Name/SHA256/First seen	Size/Type/Tags
Kopia_patnosci.xls f602: Mon, 01 Dec 2025 02:20:40 GMT	Size: 1.52 MB Type: Composite Document File V2 Document, Can't read S... document:win32:xls feed:pl-triage-new-and-malicious
Kopia_patnosci.xls af572 Sat, 29 Nov 2025 18:24:39 GMT	Size: 2.02 MB Type: ASCII text, with very long lines (65536), with no line t... document:win32:xls
Kopia_patnosci.xls b628c 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...”



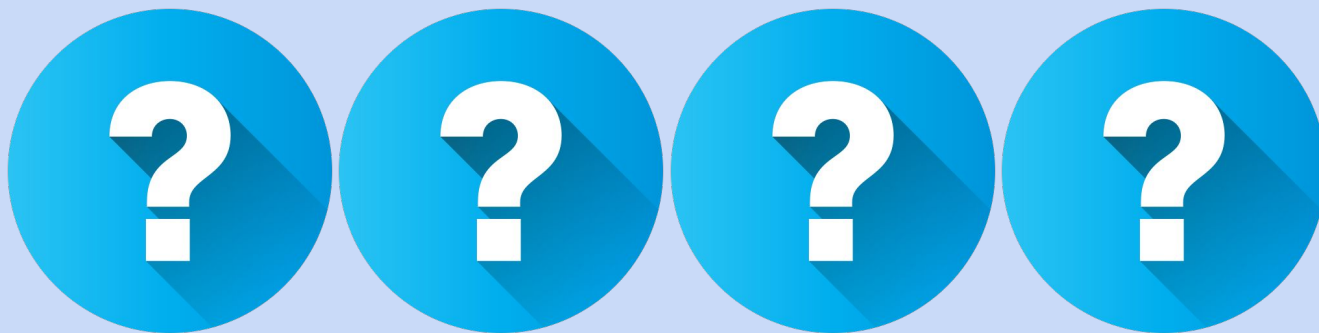
[wybierz opcję dialogową]

**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,