TLP:WHITE

jak zbierać złe dane 😈
w dobrym celu 😇

Jarosław Jedynak

Secure EB
2020-06-16

Agenda

- Kim {jestem,jesteśmy}
- Temat prezentacji
- Nasze źródła danych
- I gdzie te dane wysyłamy

$ **who**ami

Jarosław Jedynak
msm@cert.pl

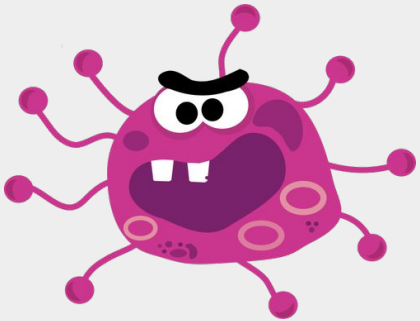
CERT.PL >_

$ **who**ami

Jarosław Jedynak
msm@cert.pl

Analiza
złośliwego
oprogramowania

CERT.PL >_

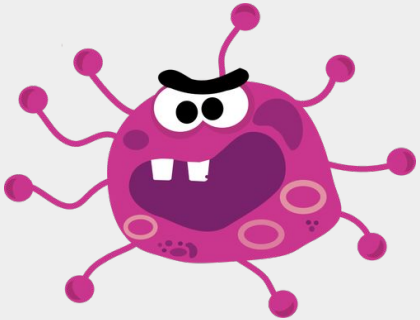


$ **who**ami

Jarosław Jedynak
msm@cert.pl

Analiza
złośliwego
oprogramowania

CERT.PL >_



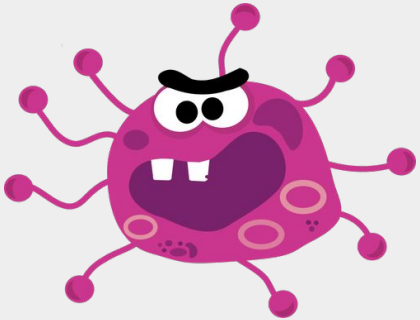
CTF @ p4.team
w “wolnym” czasie

$ **who**ami

Jarosław Jedynak
msm@cert.pl

Analiza
złośliwego
oprogramowania

CERT.PL



CTF @ p4.team
w “wolnym” czasie

Historycznie
inne zajęcia

MOBILTEK
BRILLIANT MINDS

Temat prezentacji

Czyli:
“Nie powtarzam prezentacji, ALE...

Temat prezentacji

“jak zatruć życie przestępcy”

17:20-18:00

Jak zatruć życie cyberprzestępcy? ***

Jarosław Jedynak
CERT Polska

Michał Praszmo
CERT Polska

Opis prezentacji
[UWAGA - Wystąpienie nie będzie rejestrowane!]
Jak zatruć życie cyberprzestępcy? Posyłając go za kraty, oczywiście. Niestety, nie jest to takie łatwe. Czarne charaktery utrzymujące się z nielegalnej działalności w internecie zazwyczaj bardzo dobrze dbają o bezpieczeństwo operacyjne, używają wszelkich dostępnych sposobów żeby zwiększyć swoją anonimowość, a do tego często mieszkają poza zasięgiem zachodniej policji. Nie można się jednak poddawać. Ludzie mogą być nieuchwytni, ale ich umiejętności programistyczne często pozostawiają wiele do życzenia, a ich infrastruktura bardzo często jest dziurawa. Mając odpowiednio dużo determinacji i wiedzy o bezpieczeństwie, pozwala to pozyskać z serwerów przestępców dane którymi woleliby się nie dzielić. Uzyskane informacje można następnie wykorzystać, żeby pokrzyżować złodziejom plany zanim jeszcze zaczną je realizować. Podczas prezentacji omówione zostanie kilka podatnych rodzin złośliwego oprogramowania. Skoncentrujemy się na tym, jakiego rodzaju dane można wyciągnąć, jak bezpiecznie je przetwarzać, oraz co można z nimi zrobić żeby jak najbardziej zepsuć złoczyńcom humor. Prezentację wzbogacimy ciekawostkami, zrzutami ekranów, panelami systemów i nie tylko, chociaż same szczegóły techniczne podatności będą musiały pozostać tajemnicą.

rekomendowany poziom wiedzy: ***
język prezentacji: polski
numer sali: P2R3 (Londyn 3)

Temat prezentacji

“jak zatruć życie przestępcy”

17:20-18:00 **Jak zatruć życie cyberprzestępcy?** ***

Jarosław Jedynak
CERT Polska

Michał Praszmo
CERT Polska

Opis prezentacji
[UWAGA - Wystąpienie nie będzie rejestrowane!]
Jak zatruć życie cyberprzestępcy? Posyłając go za kraty, oczywiście. Niestety, nie jest to takie łatwe. Czarne charaktery utrzymujące się z nielegalnej działalności w internecie zazwyczaj bardzo dobrze dbają o bezpieczeństwo operacyjne, używają wszelkich dostępnych sposobów żeby zwiększyć swoją anonimowość, a do tego często mieszkają poza zasięgiem zachodniej policji. Nie można się jednak [redacted] determinacji i wiedzy o bezpieczeństwie, pozwala to pozyskać z serwerów przestępców dane którymi woleliby się nie dzielić. [redacted] Podczas prezentacji omówione zostanie kilka podatnych rodzin złośliwego oprogramowania. Skoncentrujemy się na tym, jakiego rodzaju dane można wyciągnąć, jak bezpiecznie je przetwarzać, oraz co można z nimi zrobić żeby jak najbardziej zepsuć złoczyńcom humor. [redacted] szczegóły techniczne podatności będą musiały pozostać tajemnicą.

rekomendowany poziom wiedzy: ***
język prezentacji: polski
numer sali: P2R3 (Londyn 3)

CERT.PL >_

Temat prezentacji

“jak zatruć życie przestępcy”

17:20-18:00 **Jak zatruć życie cyberprzestępcy?** ***

Jarosław Jedynak
CERT Polska

Michał Praszmo
CERT Polska

Opis prezentacji
[UWAGA - Wystąpienie nie będzie rejestrowane!]
Jak zatruć życie cyberprzestępcy? Posyłając go za kraty, oczywiście. Niest[redacted]we.
Czarne charaktery utrzymujące się z nielegalnej działalności w interne[redacted]
dbają o bezpieczeństwo operacyjne, używają wszelkich dostępnych[redacted]
anonimowość, a do tego często mieszkają poza zasięgiem zachod[redacted]
[redacted]
determinacji i wiedzy o bezpieczeństwie, pozwala to pozyskać z[redacted]
woleliby się nie dzielić.
[redacted] Podczas p[redacted]
podatnych rodzin złośliwego oprogramowania. Skoncentrujemy[redacted]
można wyciągnąć, jak bezpiecznie je przetwarzać, oraz co można[redacted]
zepsuć złoczyńcom humor.
[redacted] szczegóły techniczne podatności[redacted]
tajemnicą.

rekomendowany poziom wiedzy: ***
język prezentacji: polski
numer sali: P2R3 (Londyn 3)

CERT.PL >_

Temat prezentacji

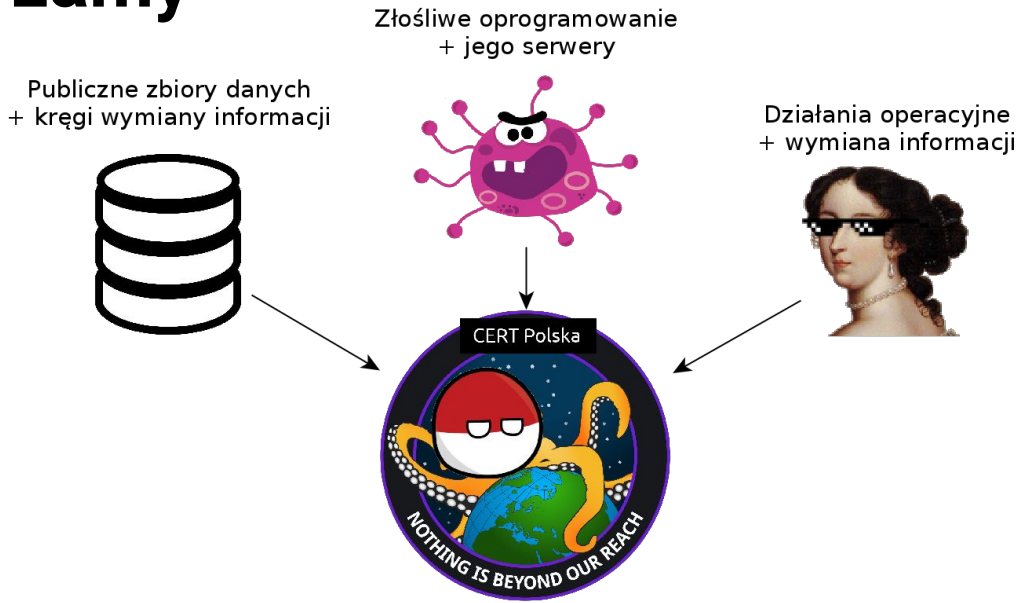
~~“jak zatruć życie przestępcy”~~

jak zbierać dane

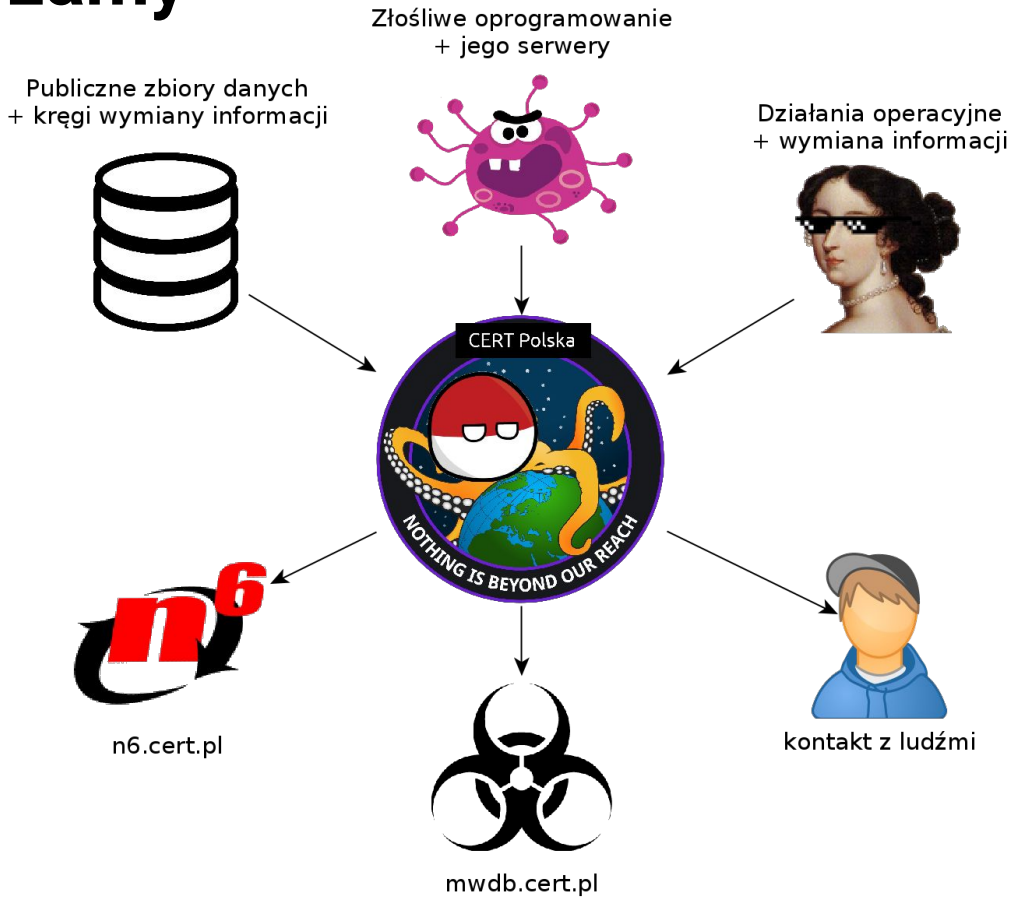
Dokąd zmierzamy

CERT.PL >_

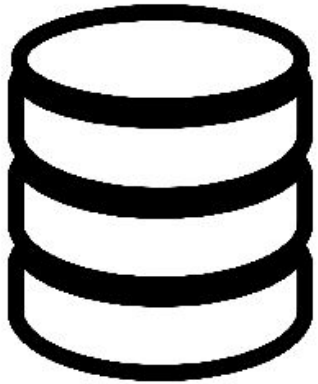
Dokąd zmierzamy



Dokąd zmierzamy



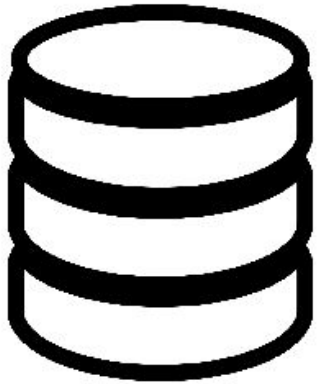
Źródła: Publiczne zbiory danych



- Hasze złośliwego oprogramowania
- Próbki złośliwego oprogramowania
- Złośliwe URL
- Złośliwe domeny
- Czasami dodatkowe metadane

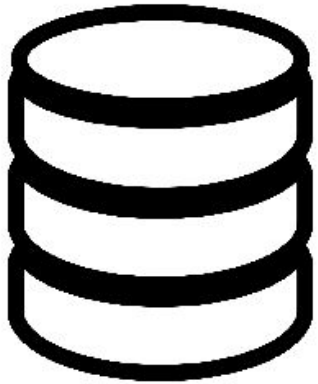
Źródła: Publiczne zbiory danych

- URLhaus 💖 (https://urlhaus.abuse.ch/)



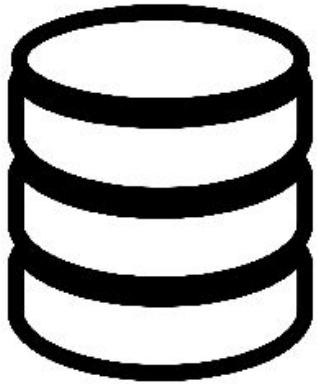
Źródła: Publiczne zbiory danych

- URLhaus 💖 (https://urlhaus.abuse.ch/)
- MalwareBazaar (https://bazaar.abuse.ch/)

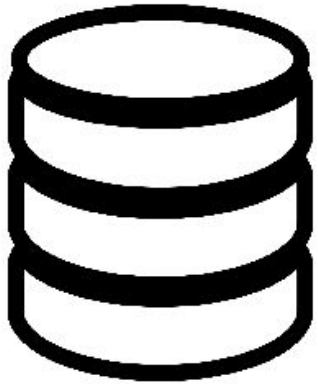


Źródła: Publiczne zbiory danych

- URLhaus 💖 (https://urlhaus.abuse.ch/)
- MalwareBazaar (https://bazaar.abuse.ch/)
- abuse.ch (https://abuse.ch)



Źródła: Publiczne zbiory danych



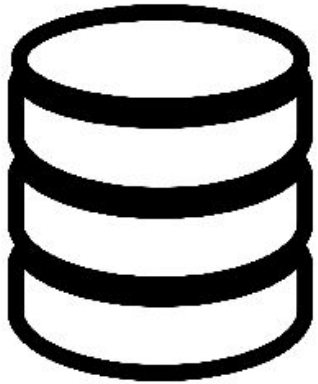
- URLhaus 💖 (https://urlhaus.abuse.ch/)
- MalwareBazaar (https://bazaar.abuse.ch/)
- abuse.ch (https://abuse.ch)
- VxUnderground

URLhaus by ABUSE.ch

MALWARE bazaar by ABUSE.ch

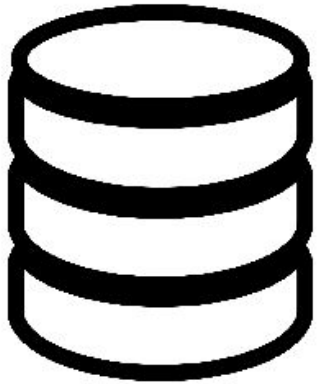
ABUSE.ch

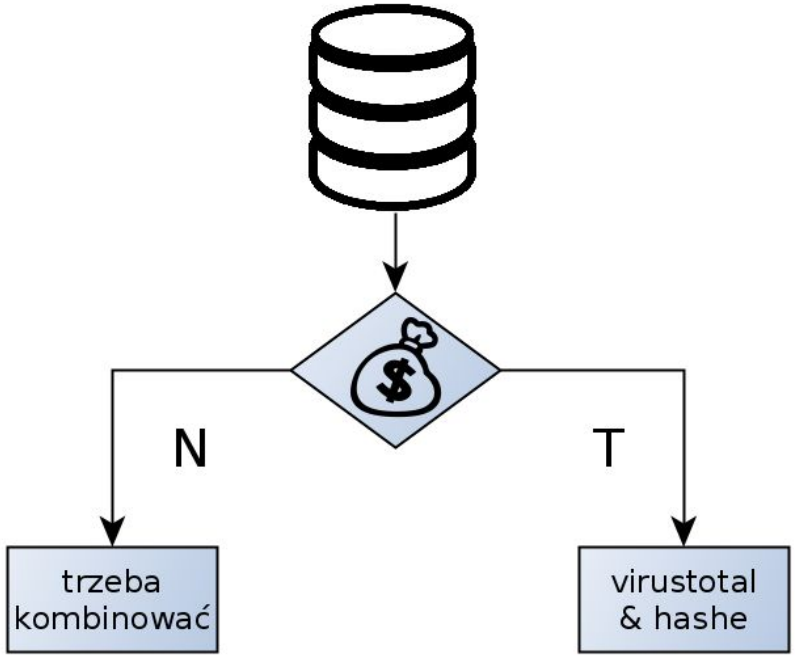
Źródła: Publiczne zbiory danych



- URLhaus 💖 (https://urlhaus.abuse.ch/)
- MalwareBazaar (https://bazaar.abuse.ch/)
- abuse.ch (https://abuse.ch)
- VxUnderground
- VirusShare

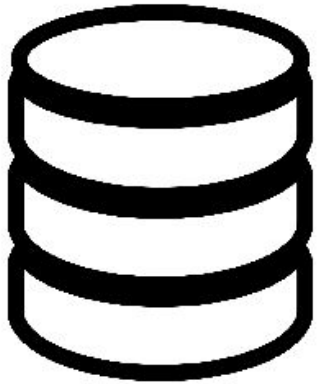
Źródła: Publiczne zbiory danych





(dla analityków, nie blacklist)

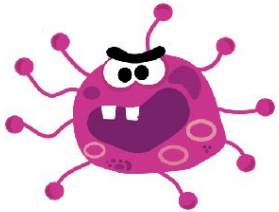
Źródła: Publiczne zbiory danych

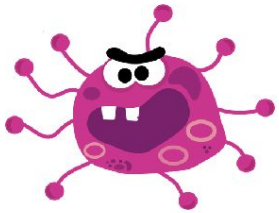


URLhaus database dump (CSV) containing only **online** (active) malware URLs:

Download CSV (online URLs only)

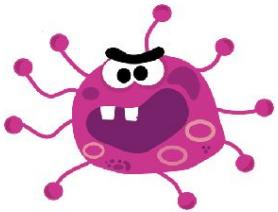
Źródła: Publiczne zbiory danych

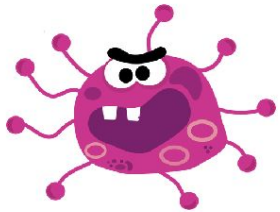




URLhaus database dump (CSV) containing only **online** (active) malware URLs:

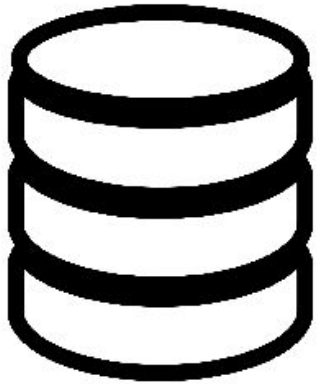
Do ne URLs only)





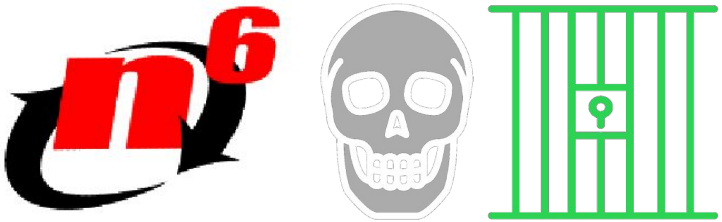
CERT.PL >_

Źródła: Publiczne zbiory danych



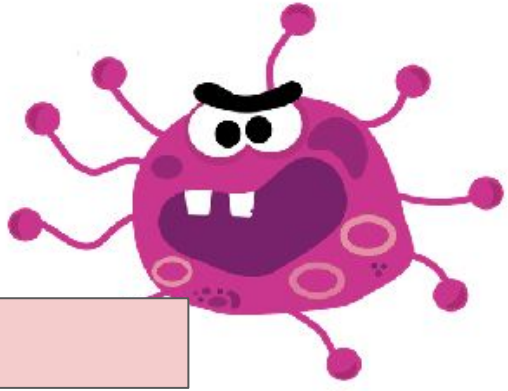
- URLhaus 💖 (https://urlhaus.abuse.ch/)
- MalwareBazaar (https://bazaar.abuse.ch/)
- abuse.ch (https://abuse.ch)
- VxUnderground
- VirusShare

- n6 (https://n6.cert.pl)
- mwdb (https://mwdb.cert.pl)



CERT.PL >_

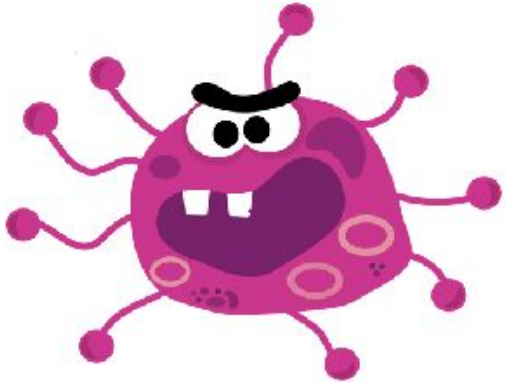
Źródła: Złośliwe oprogramowanie



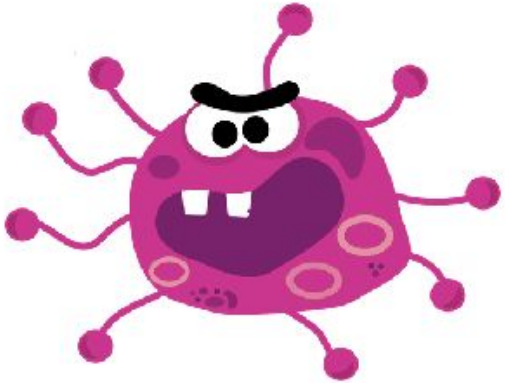
- Więcej próbek złośliwego oprogramowania
- URLe i domeny serwerów C2
- Klucze do komunikacji
- Identyfikatory kampanii
- Konfiguracja kampanii
- Szablony wiadomości spamowych
- IP innych peerów w botnecie
- Pliki z żądeniem okupu
- Zaszyte hardkodowane hasła

Źródła: Złośliwe oprogramowanie

Czyli “o tym już chyba była prezentacja”



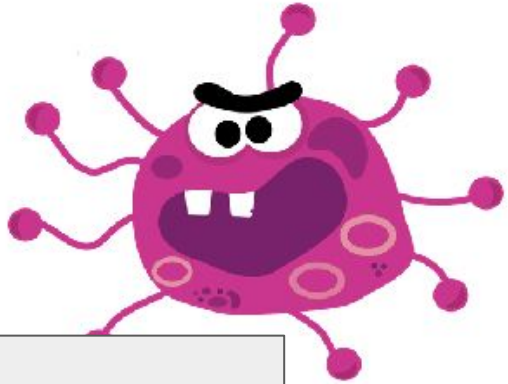
Źródła: Złośliwe oprogramowanie



Czyli “o tym już chyba była prezentacja”

Jarosław Jedynak, Paweł Srokosz.
"Use your enemies: tracking botnets with bots"

Źródła: Złośliwe oprogramowanie



Czyli “o tym już chyba była prezentacja”

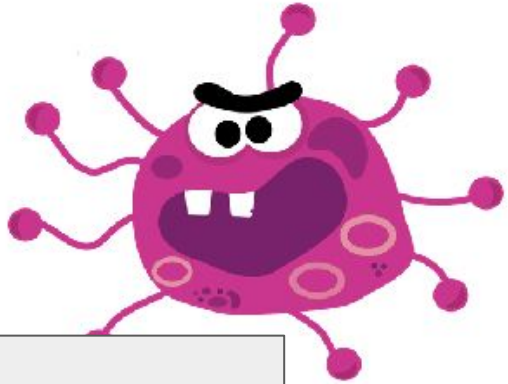
Łukasz Siewierski
“(Mostly) Polish threat landscape: not only VBKlip”

Jarosław Jedynak, Paweł Srokosz.
"Use your enemies: tracking botnets with bots"

Łukasz Siewierski, "Middle Income Malware Actors in Poland: VBKlip and Beyond”

CERT.PL >_

Źródła: Złośliwe oprogramowanie



Czyli “o tym już chyba była prezentacja”

Maciej Kotowicz
“ISFB, Still Live and Kicking”

Łukasz Siewierski
“(Mostly) Polish threat landscape: not only VBKlip”

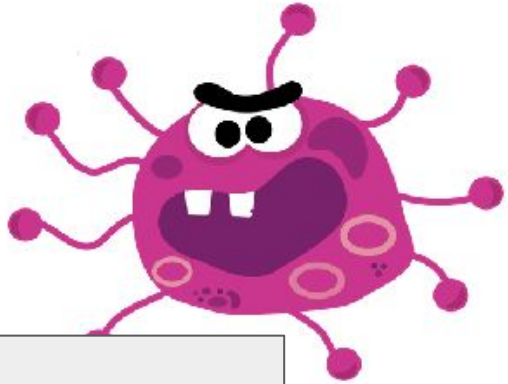
Jarosław Jedynak, Paweł Srokosz.
"Use your enemies: tracking botnets with bots"

Maciej Kotowicz
“ZeuS meets VM, story so far”

Maciej Kotowicz
"Malware Calling”

Łukasz Siewierski, "Middle Income Malware Actors in Poland: VBKlip and Beyond”

Źródła: Złośliwe oprogramowanie



Czyli “o tym już chyba była prezentacja”

Maciej Kotowicz
“ISFB, Still Live and Kicking”

Łukasz Siewierski
“(Mostly) Polish threat landscape: not only VBKlip”

Jarosław Jedynak, Paweł Srokosz.
"Use your enemies: tracking botnets with bots"

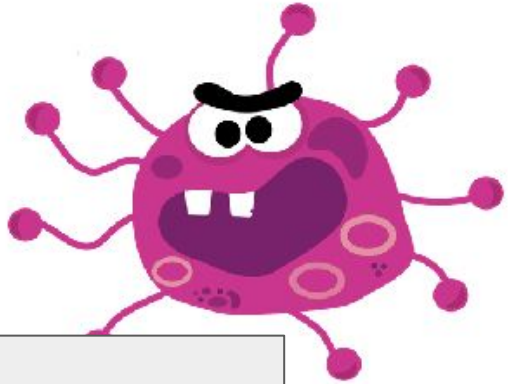
Maciej Kotowicz
“ZeuS meets VM, story so far”

Maciej Kotowicz
"Malware Calling”

Piotr Białczak, “Leaving no Stone Unturned – in Search of HTTP Malware Distinctive Features”

Łukasz Siewierski, "Middle Income Malware Actors in Poland: VBKlip and Beyond”

Źródła: Złośliwe oprogramowanie



Czyli “o tym już chyba była prezentacja”

Maciej Kotowicz
“ISFB, Still Live and Kicking”

Łukasz Siewierski
“(Mostly) Polish threat landscape: not only VBKlip”

Jarosław Jedynak, Maciej Kotowicz
“Nymaim, the untold story”

ak, Paweł Srokosz.
ies: tracking botnets with bots"

Jarosław Jedynak, Maciej Kotowicz
“Peering into spambotnets”

Michał Leszczyński, Krzysztof Stopczański
“Hypervisor-level malware monitoring and extraction system”

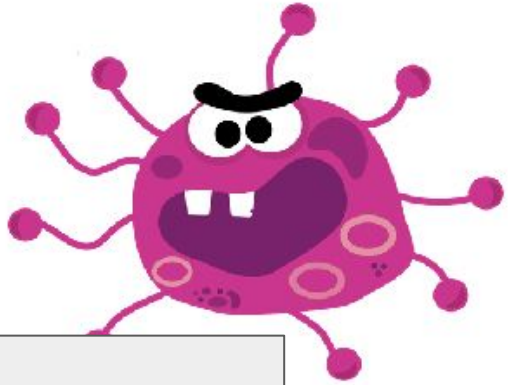
“ZeuS meets VM, story so far”

"Malware Calling”

Piotr Białczak, “Leaving no Stone Unturned – in Search of HTTP Malware Distinctive Features”

Łukasz Siewierski, "Middle Income Malware Actors in Poland: VBKlip and Beyond”

Źródła: Złośliwe oprogramowanie



Czyli “o ty… …tacja”

Tomasz Bukowski
“ZitMo - case study”

Maciej Kotowicz
“ISFB, Still Live and Kicking”

Łukasz Siewierski
“(Mostly) Polish threat lan…

Tomasz Sałaciński
“Techniki anti-reversing w botach SpyEye”

Jarosław Jedynak, Maciej Kotowicz
“Peering into spambotnets”

Paweł Jacewicz, Łukasz Juszczyk
“Anatomia złośliwego PDFa”

…ak, Paweł Srokosz.
…es: tracking botnets with bots"

Michał Leszczyński, Krzysztof Stopczański
“Hypervisor-level malware monitoring and extraction system”

“ZeuS meets VM, story…

Tomasz Bukowski, Tomasz Sałaciński
“Analiza Spyware - SpyeEye i Zeus”

Piotr Białczak, “Leaving no Stone Unturned – In…

Łukasz Siewierski, "Middle Income Malware Actors in Poland: VBKlip and Be…

Paweł Krześniak
“Wykrywanie podejrzanych domen internetowych poprzez pasywną analizę ruchu DNS”

Piotr Kijewski
“Platforma n6”

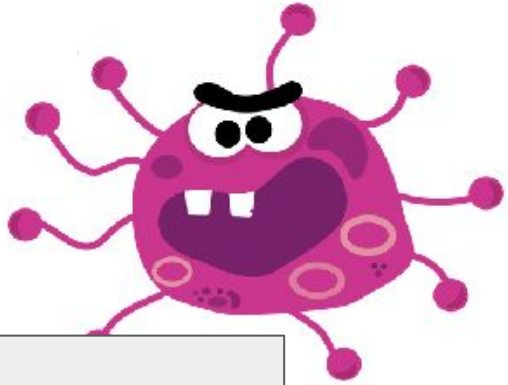
Źródła: Złośliwe oprogramowanie

secure 2011

Tomasz Bukowski
“ZitMo - case study”

Czyli “o ty… …tacja”

virus BULLETIN



Maciej Kotowicz
“ISFB, Still Live and Kicking”

Łukasz Siewierski
“(Mostly) Polish threat lan…

Tomasz Sałaciński
“Techniki anti-reversing w botach SpyEye”

Jarosław Jedynak, Maciej Kotowicz

Paweł Jacewicz, Łukasz Juszczyk
“Anatomia złośliwego PDFa”

…ak, Paweł Srokosz.
…es: tracking botnets with bots"

Jarosław Jedynak, Maciej Kotowicz
“Peering into spambotnets”

Michał Leszczyński, Krzysztof Stopczański
“Hypervisor-level malware monitoring and extraction system”

“ZeuS meets VM, story…

Tomasz Bukowski, Tomasz Sałaciński
“Analiza Spyware - SpyeEye i Zeus”

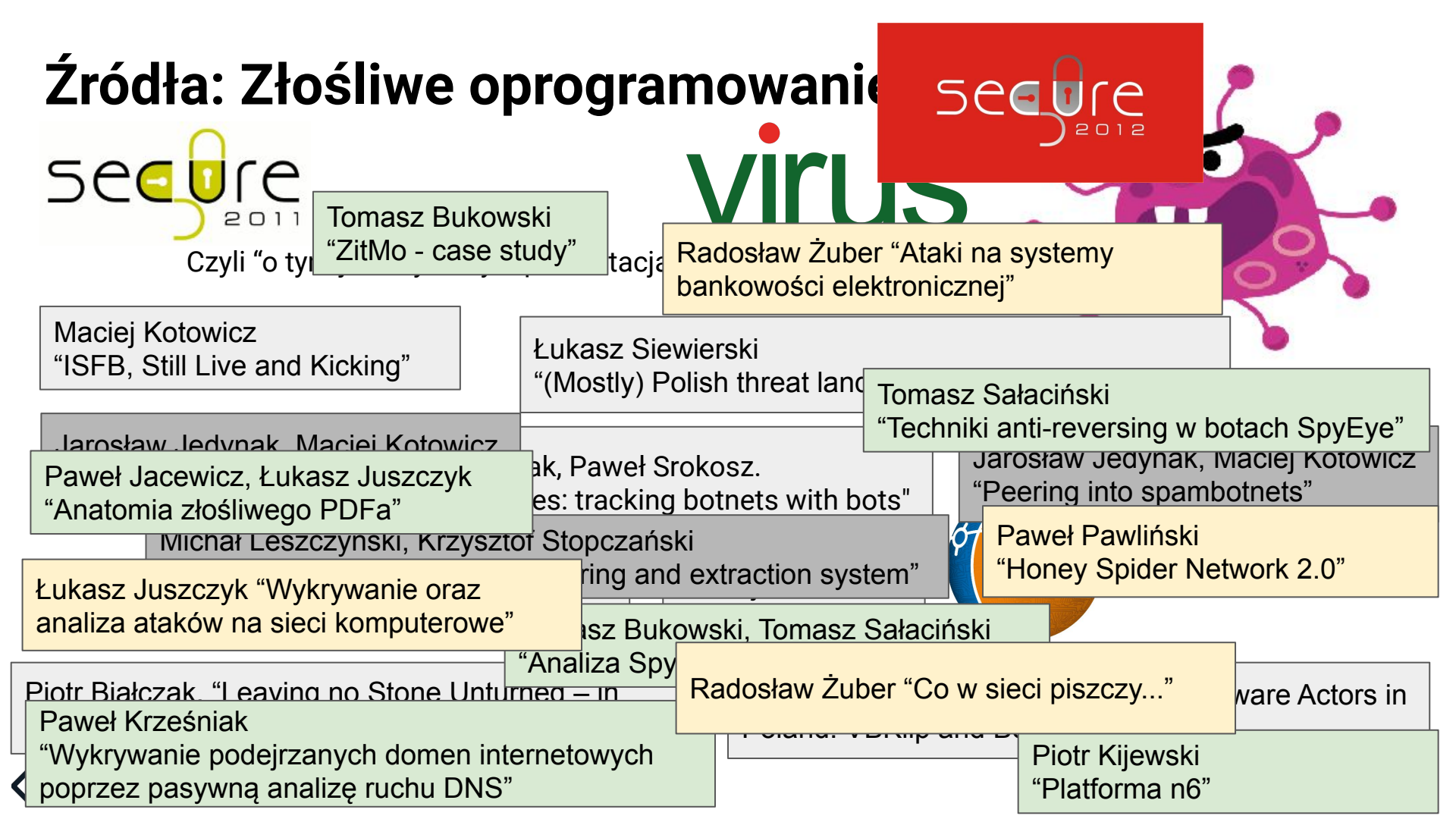
Piotr Białczak, “Leaving no Stone Unturned – In…

Łukasz Siewierski, "Middle Income Malware Actors in Poland: VBKlip and Be…

Paweł Krześniak
“Wykrywanie podejrzanych domen internetowych poprzez pasywną analizę ruchu DNS”

Piotr Kijewski
“Platforma n6”

Źródła: Złośliwe oprogramowanie



Źródła: Złośliwe oprogramowanie

secure 2012

secure 2011

Tomasz Grudziecki, Paweł Jacewicz "Intruz w sieci. Wykrywanie i analiza ataków oraz infekcji w sieciach korporacyjnych

Tomasz B
"ZitMo - case study

Czyli "o ty tacja

Radosław Zuber "Ataki na systemy bankowości elektronicznej"

secure 2013

Maciej Kotowicz
"ISFB, Still Live a

Łukasz Siewierski
ish threat land

Piotr Kijewski
"CERT Polska vs botnety"

Tomasz Sałaciński
"Techniki anti-reversing w botach SpyEye"

Jarosław Jedynak, Maciej Kotowicz

ak, Paweł Srokosz.
es: tracking botnets with bots"

Jarosław Jedynak, Maciej Kotowicz
"Peering into spambotnets"

Paweł Jacewicz, Łukasz Juszczyk
"Anatomia złośliwego PDFa"

Michał Leszczyński, Krzysztof Stopczański
ring and extr

Paweł Pawliński
r Network 2.0"

Łukasz Juszczyk "Wykrywanie oraz analiza ataków na sieci komputerowe"

Paweł Pawliński
"n6: otwarta wymiana danych"

asz Bukowsk

Tomasz Bukowski, Łukasz Siewierski
"Wyszukiwanie i identyfikacja śladów infekcji złośliwym oprogramowaniem"

piszczy..."

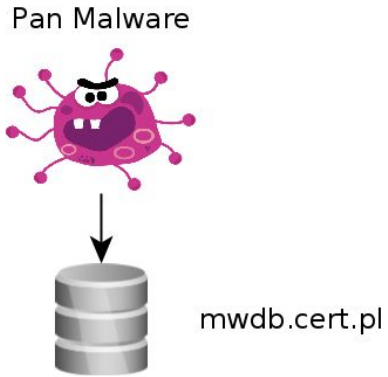
ware Actors in

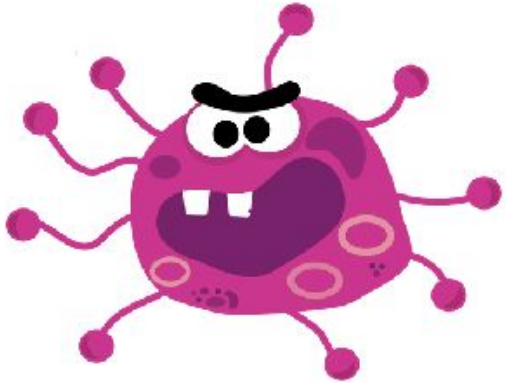
"Wykrywanie podejrzanych domen internetowych poprzez pasywną analizę ruchu DNS"

Piotr Kijewski
"Platforma n6"

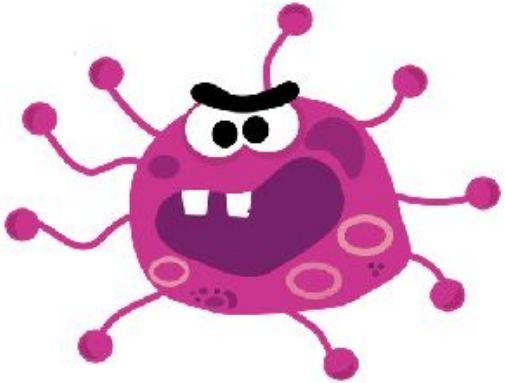
Źródła: Złośliwe oprogramowanie

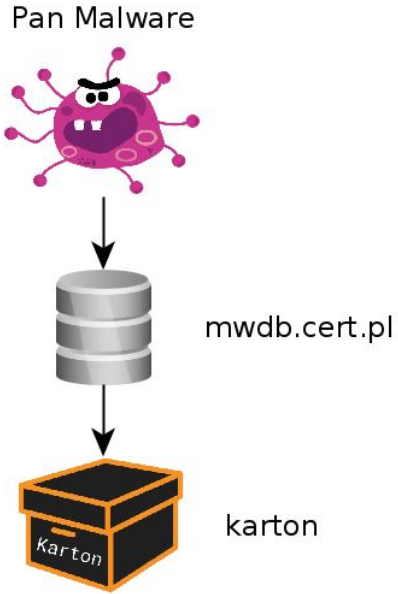
Źródła: Złośliwe oprogramowanie



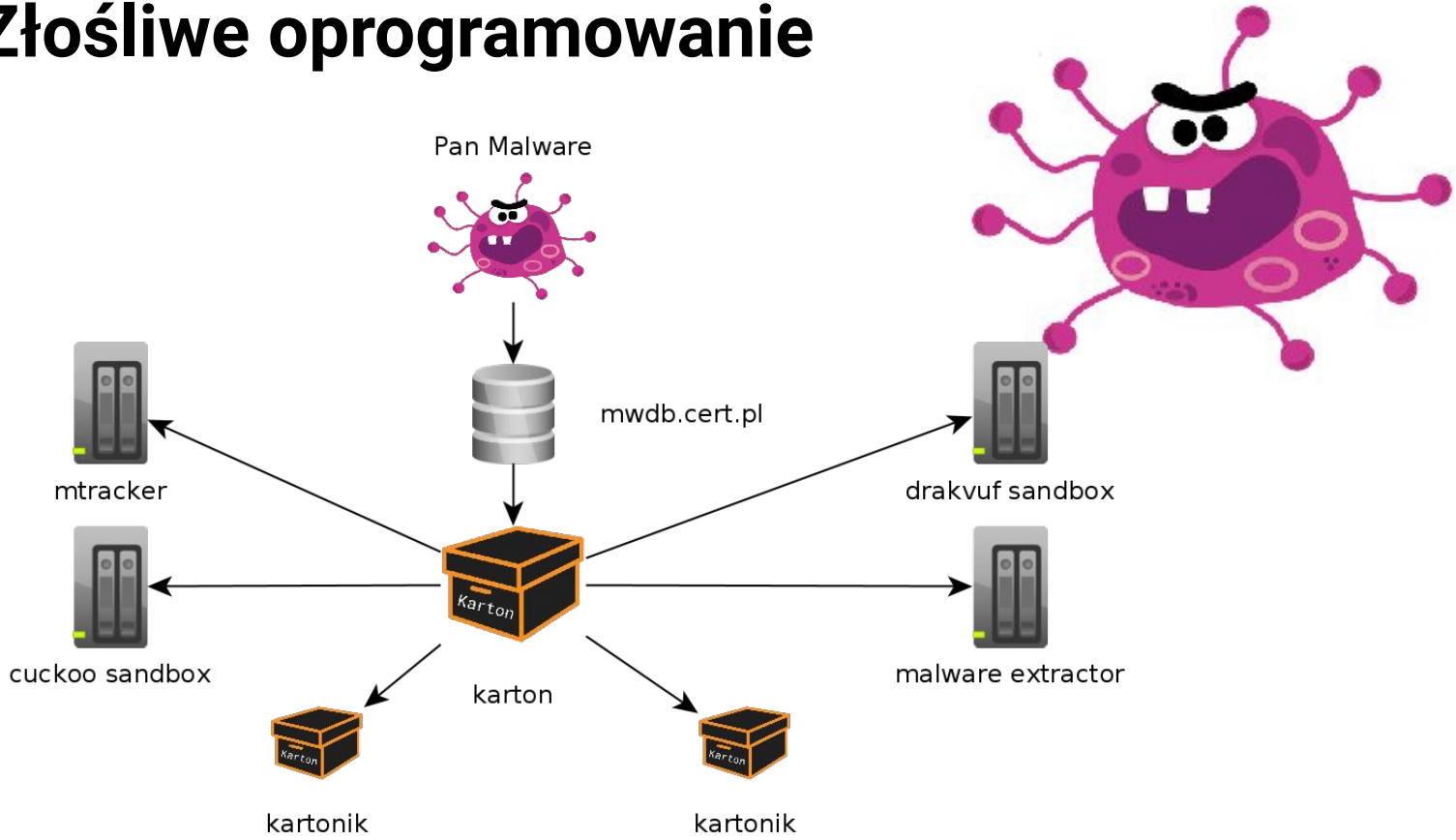


Źródła: Złośliwe oprogramowanie

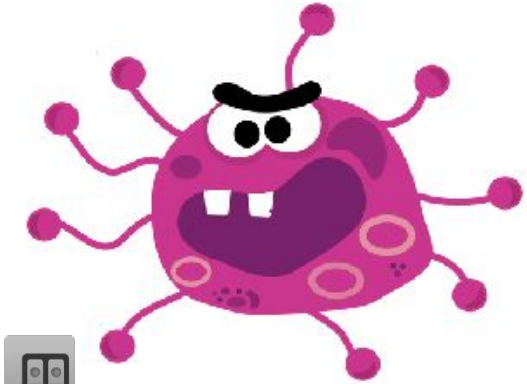


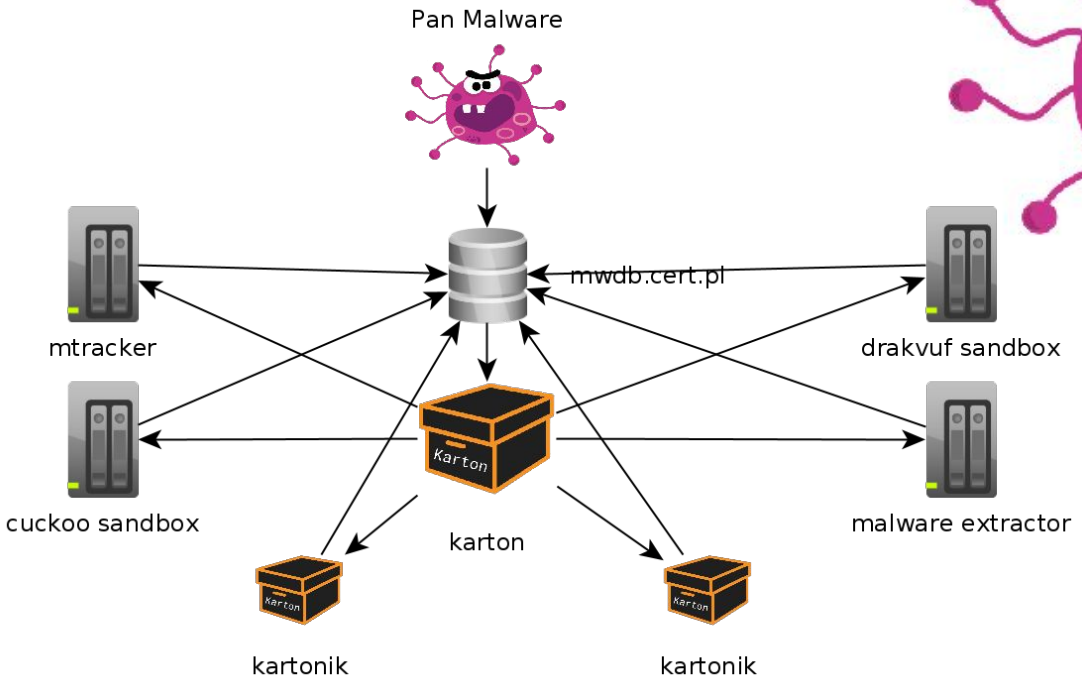


Źródła: Złośliwe oprogramowanie



Źródła: Złośliwe oprogramowanie



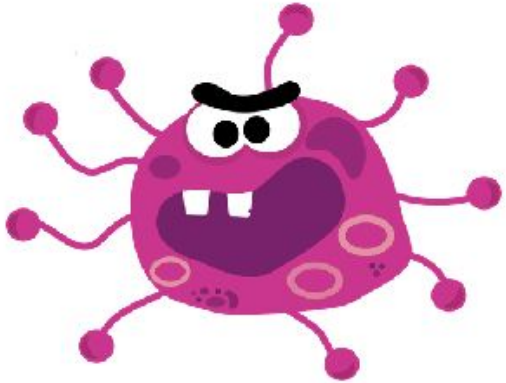


CERT.PL

Źródła: Złośliwe oprogramowanie

```
from ripper import Extractor

class Citadel(Extractor):
    family = "citadel"
    yara_rules = ["citadel"]
    overrides = ["zeus"]

    @Extractor.extractor("briankerbs")
    def citadel_found(self, p, addr):
        log.info('[+] `Coded by Brian Krebs` str @ %X' % addr)
        return True

    @Extractor.extractor
    def cit_login(self, p, addr):
        log.info('[+] Found login_key xor @ %X' % addr)
        hit = p.uint32v(addr + 4)
        print(hex(hit))
        if p.is_addr(hit):
            return {'login_key': p.asciiz(hit)}

        hit = p.uint32v(addr + 5)
        print(hex(hit))
        if p.is_addr(hit):
            return {'login_key': p.asciiz(hit)}
```

https://malduck.readthedocs.io



Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

- Jeszcze więcej próbek złośliwego oprogramowania
- Wykradzione dane logowania
- Wykradzione numery kart
- Dane na temat infrastruktury
- Różne inne ciekawe rzeczy?

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

Jeszcze więcej próbek złośliwego oprogramowania

Wykradzione dane logowania

Wykradzione numery kart

Dane na temat infrastruktury

Inne ciekawe informacje

mwdb.cert.pl

Wysyłane “wybiórczo”

Wykorzystywane wewnętrznie

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

(Jak Zatruć Życie Cyberprzestępcy)

Wysyłane “wybiórczo”

Wykorzystywane wewnętrznie

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

Społeczność, administratorzy usług, etc

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

CERT.PL >_ Zgłoś incydent PL EN

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.

Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

- Osoba fizyczna / inne podmioty
- Operator usług kluczowych
- Dostawca usługi cyfrowej
- Podmiot publiczny

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

CERT.PL >_ Zgłoś incydent PL EN

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.

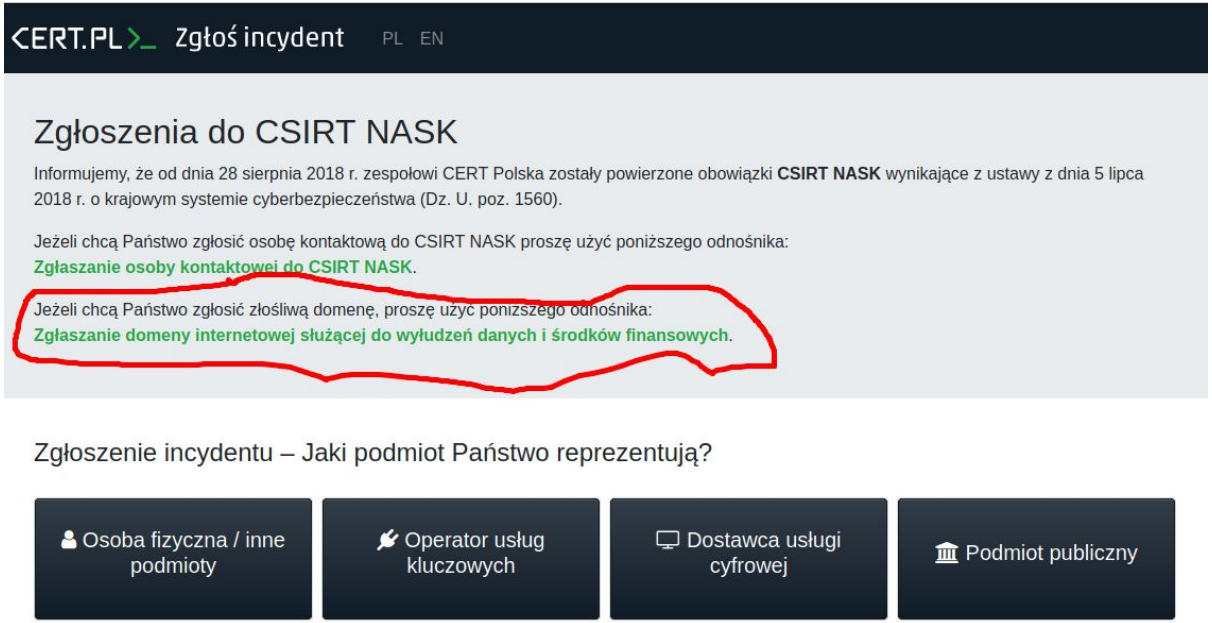
Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

- Osoba fizyczna / inne podmioty
- Operator usług kluczowych
- Dostawca usługi cyfrowej
- Podmiot publiczny

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych



Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

Prosimy o wypełnienie poniższego formularza

Złośliwe domeny

W ramach zgłoszenia można wskazać maksymalnie 50 złośliwych domen.

Złośliwe domeny lub adresy URL (po jednym w linii)

Uzasadnienie zgłoszenia

CERT.PL

Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych

Zgłaszanie podejrzanych stron

Każdy może zgłosić stronę, która może wyłudzać dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych, za pomocą formularza dostępnego na https://incydent.cert.pl/phishing.

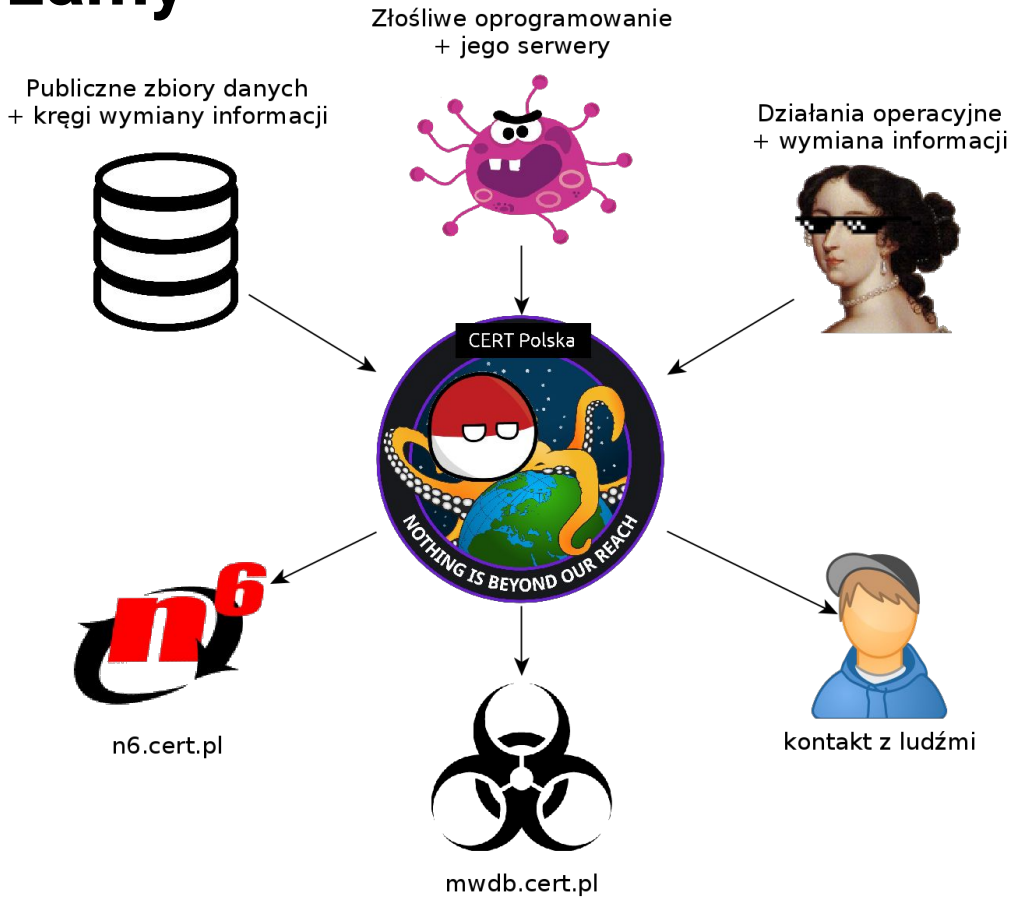
Lista ostrzeżeń

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie dostępna jest jako następujące pliki:

- format tekstowy, tylko aktywne domeny, jedna domena per linia: https://hole.cert.pl/domains/domains.txt
- format TSV (tab-separated values): https://hole.cert.pl/domains/domains.csv
- format JSON: https://hole.cert.pl/domains/domains.json
- format XML: https://hole.cert.pl/domains/domains.xml

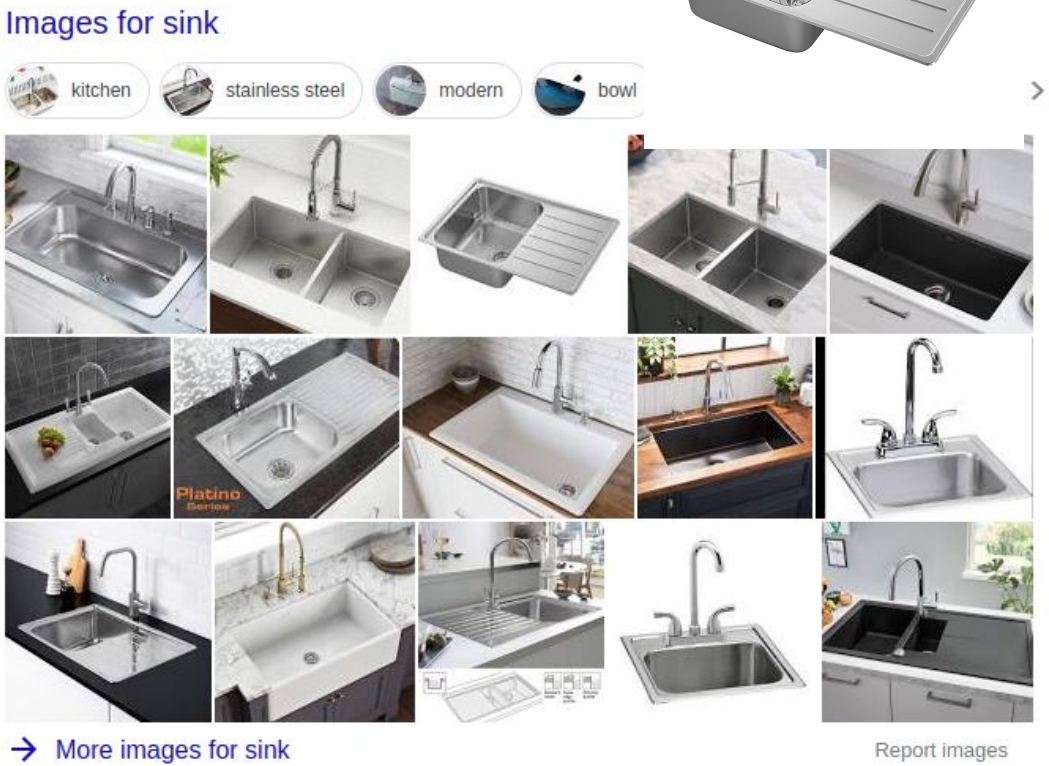
Pliki są aktualizowane co 5 minut. Pełna specyfikacja naszego API dostępna jest tutaj.

Dokąd zmierzamy



Dygresja językowa: “sink”?

Source -> Sink
Źródło -> ???



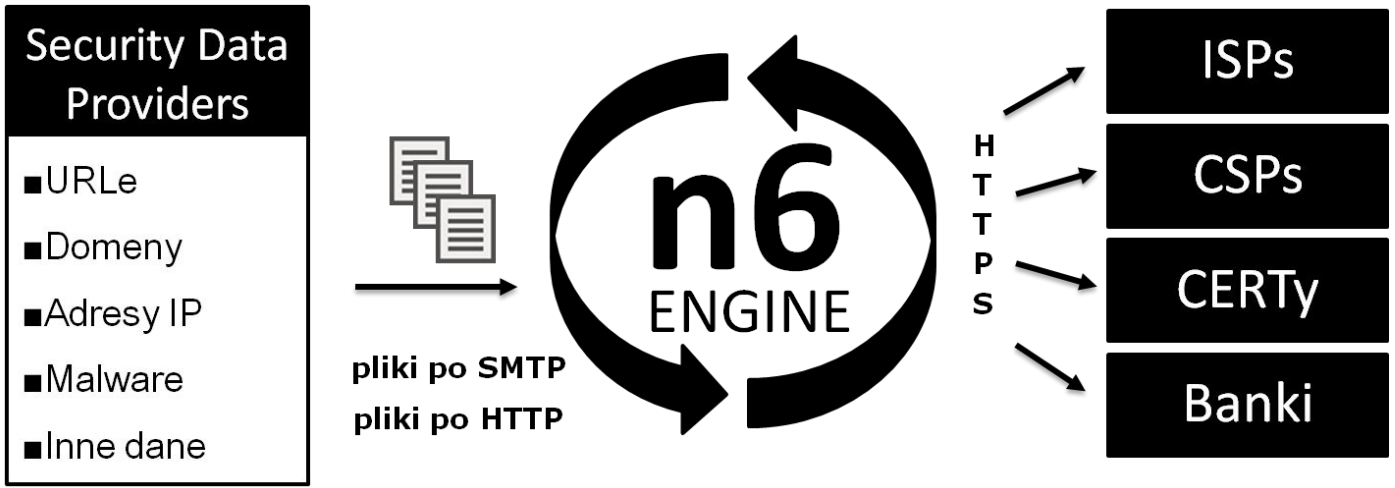
CERT.PL

Ujście: n6

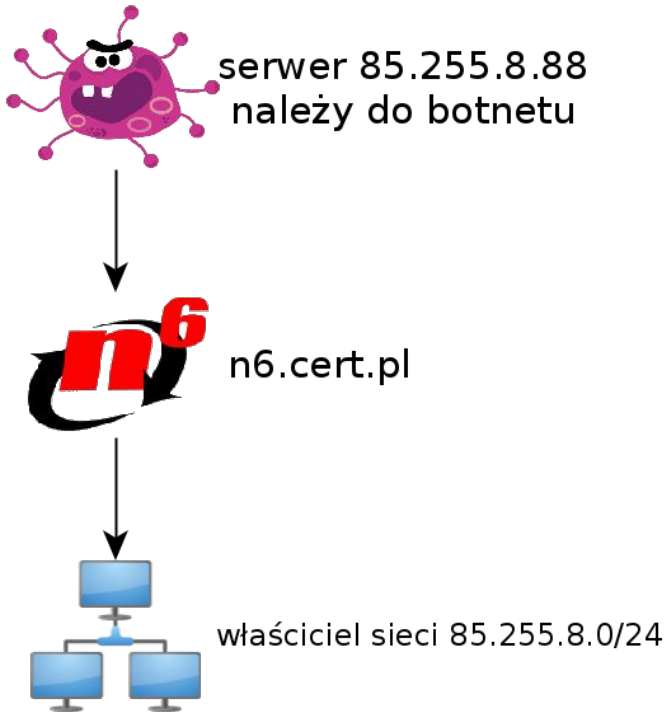
Dostępne dla: administratorów sieci, CERTów.

Dane: informacje o incydentach.

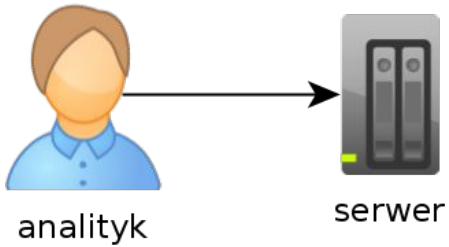
Ujście: n6


Security Data Providers
■URLe
■Domeny
■Adresy IP
■Malware
■Inne dane
pliki po SMTP
pliki po HTTP
n6
ENGINE
HTTPS
ISPs
CSPs
CERTy
Banki

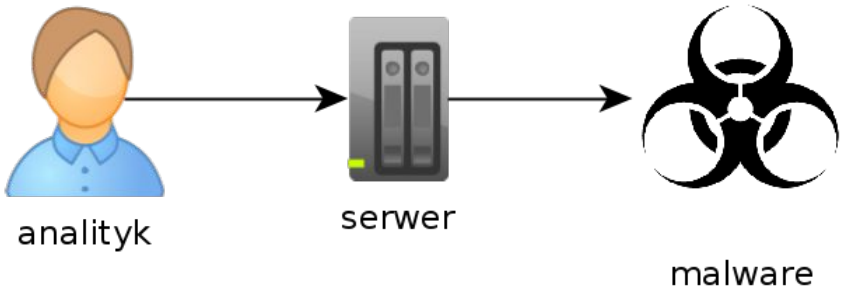
Ujście: n6


serwer 85.255.8.88
należy do botnetu
n6.cert.pl
właściciel sieci 85.255.8.0/24

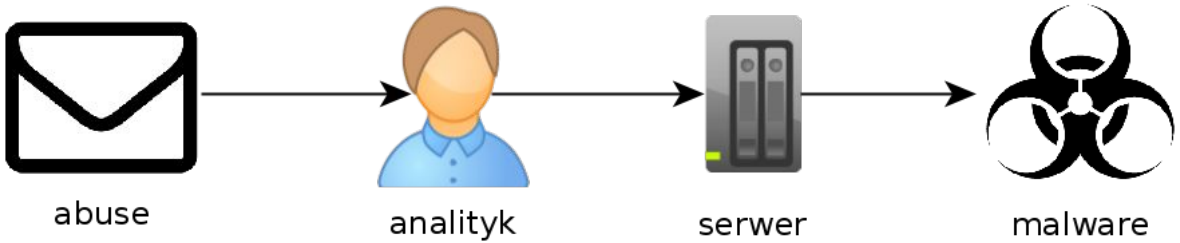
Dygresja: Przepływ danych



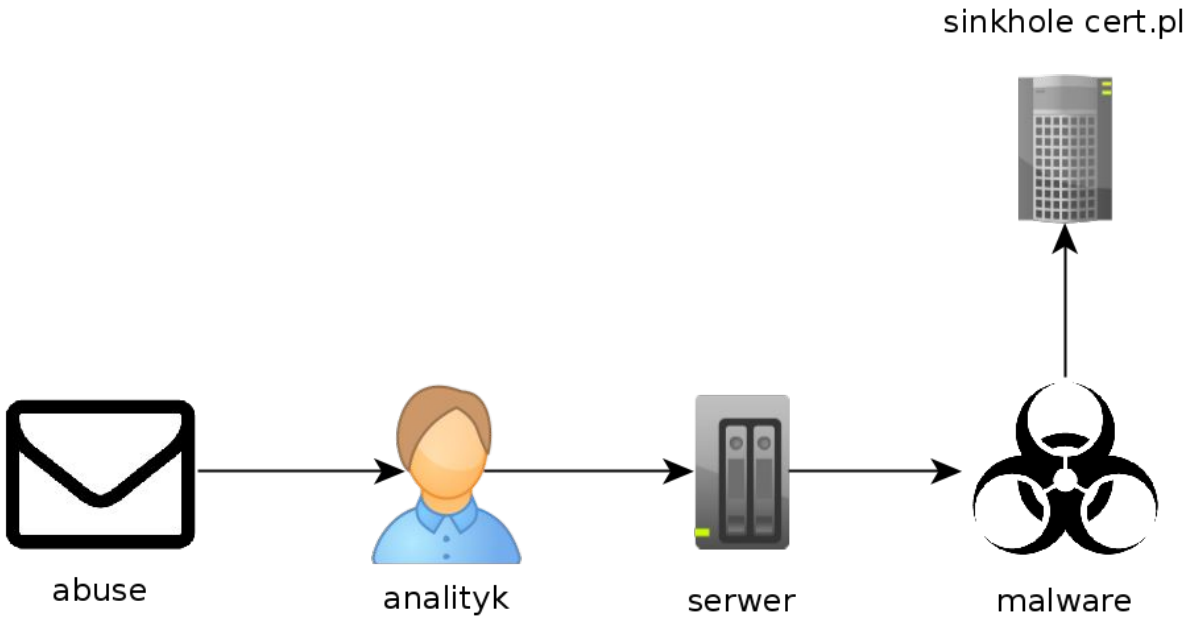
Dygresja: Przepływ danych



Dygresja: Przepływ danych

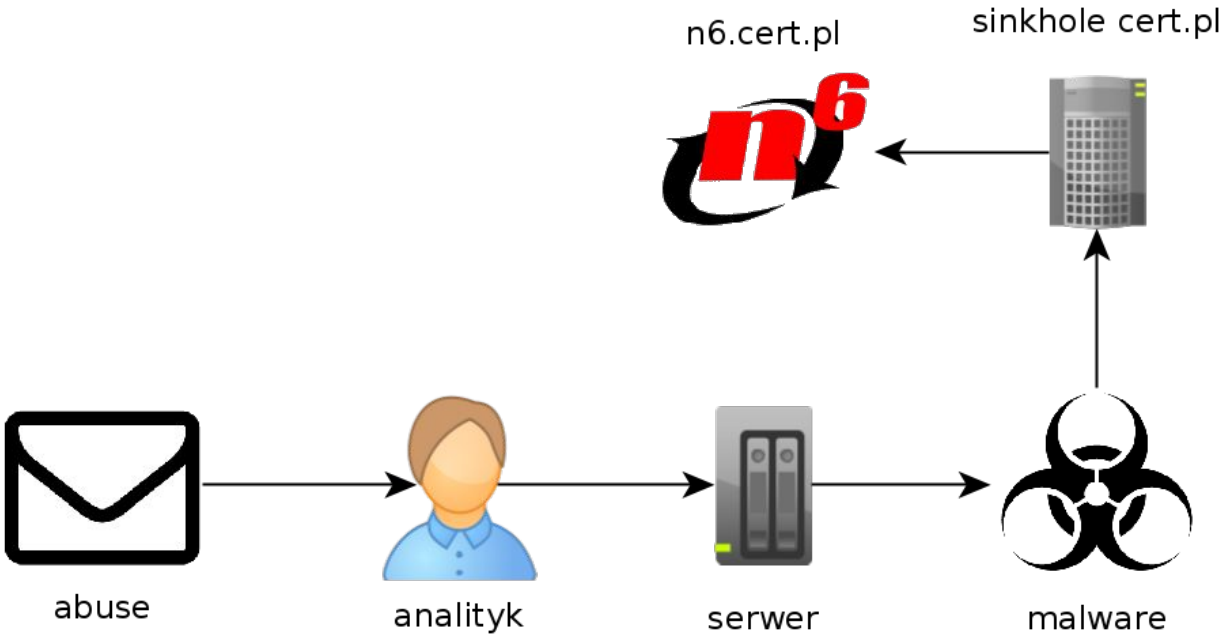


Dygresja: Przepływ danych

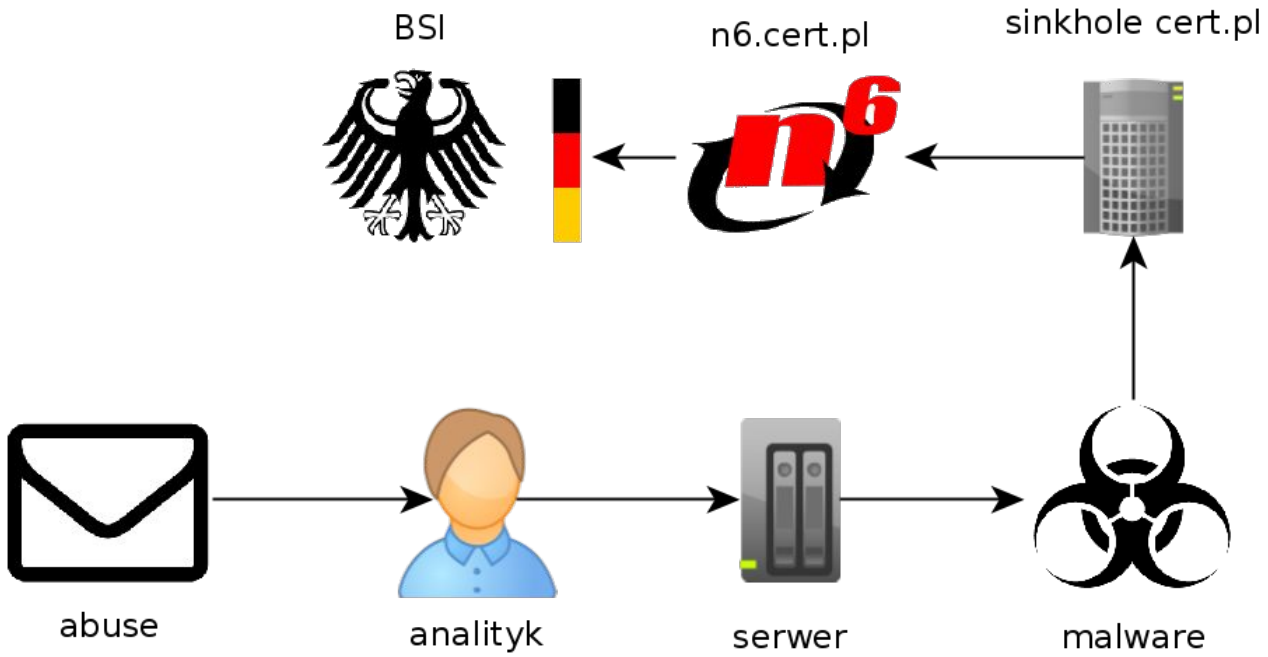


CERT.PL

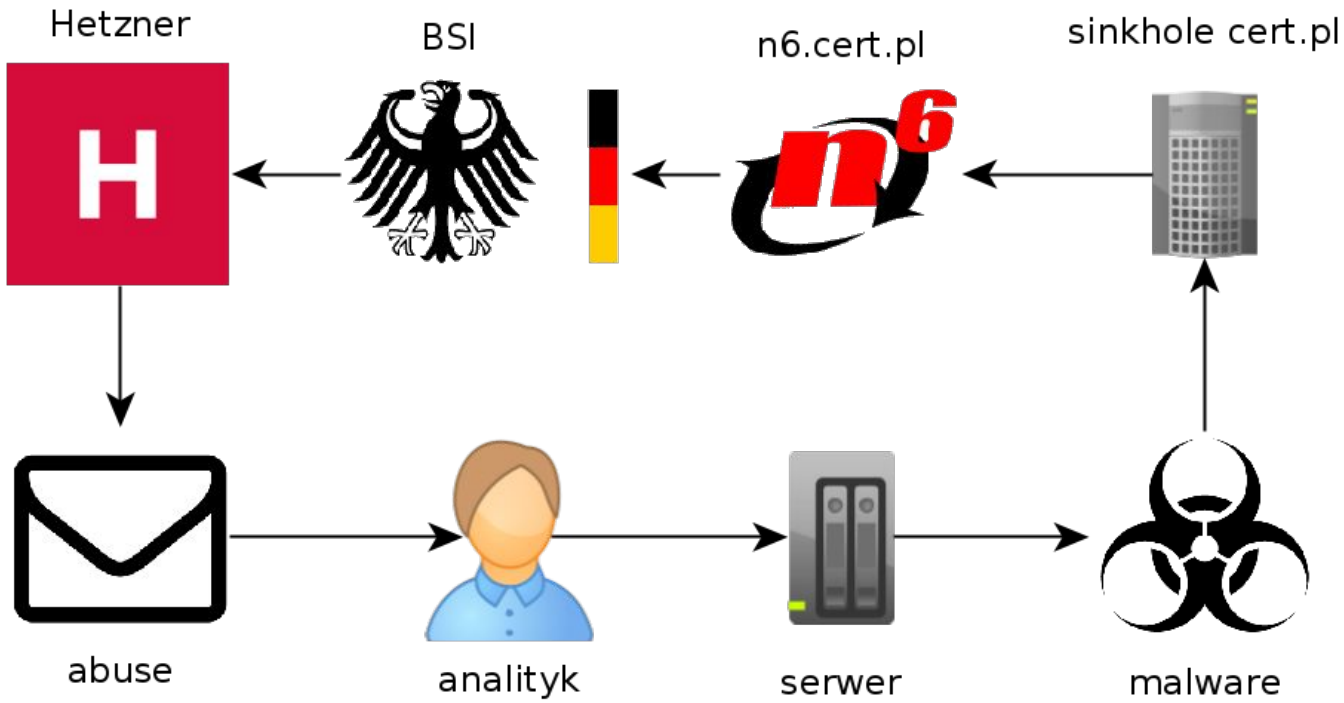
Dygresja: Przepływ danych



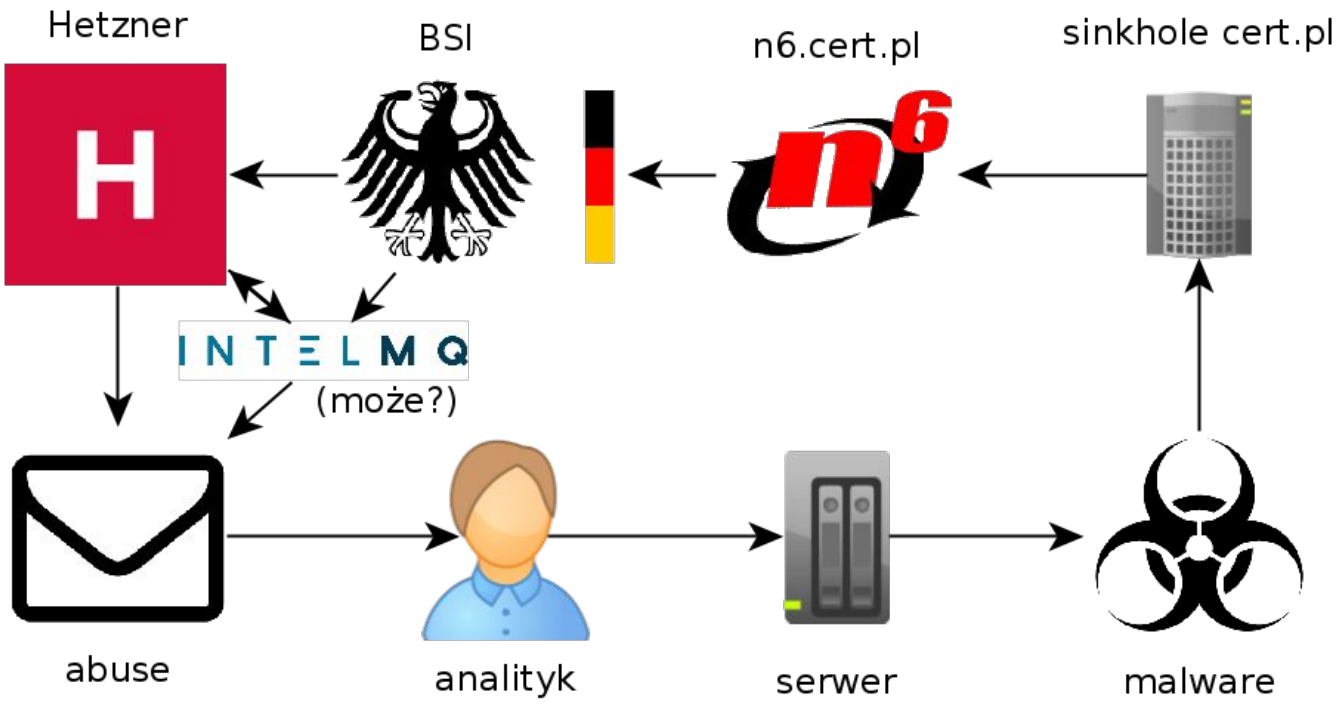
Dygresja: Przepływ danych



Dygresja: Przepływ danych



Dygresja: Przepływ danych

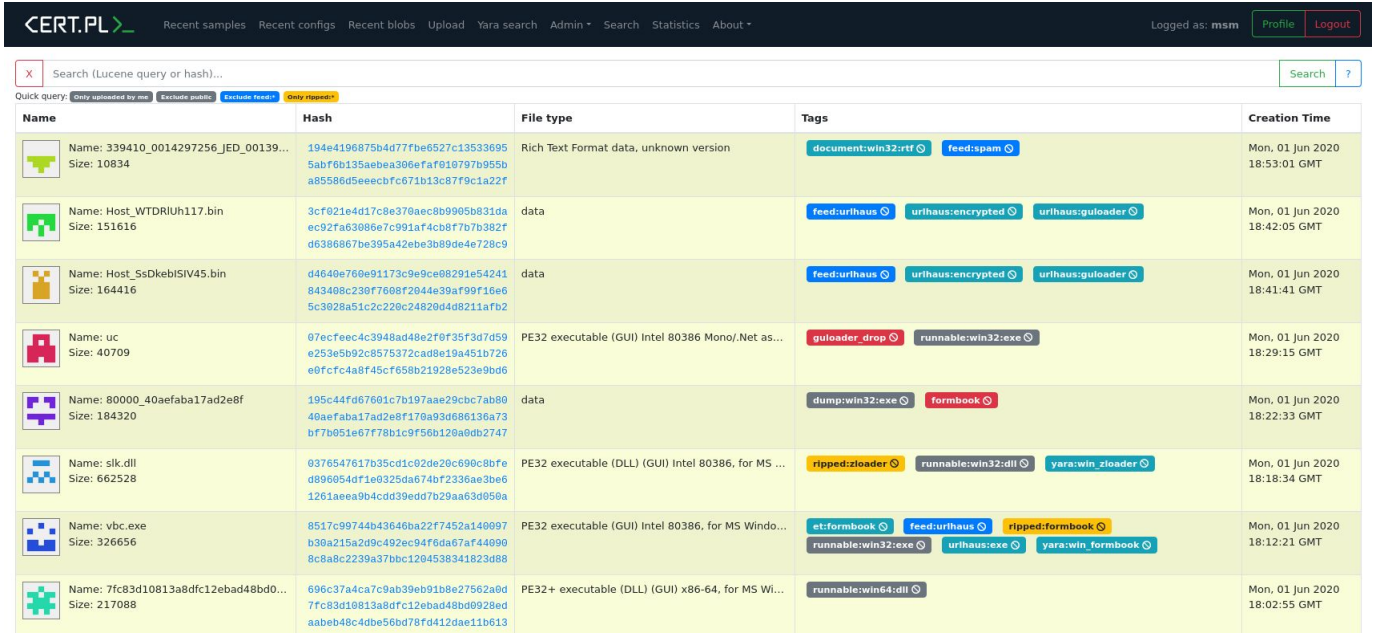


Ujście: mwdb

Dostępne dla: analityków malware

Dane: informacje o próbkach.

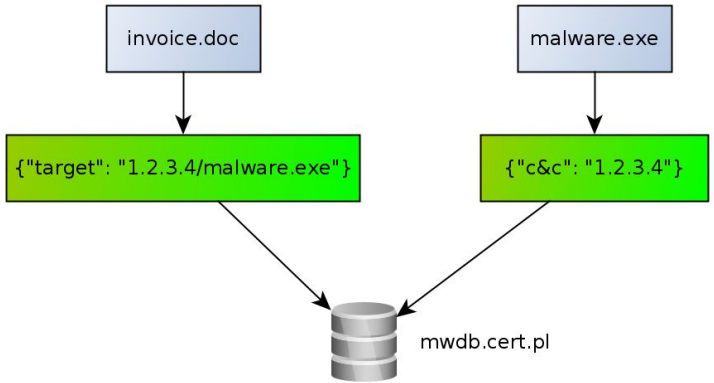
Ujście: mwdb.cert.pl



CERT.PL

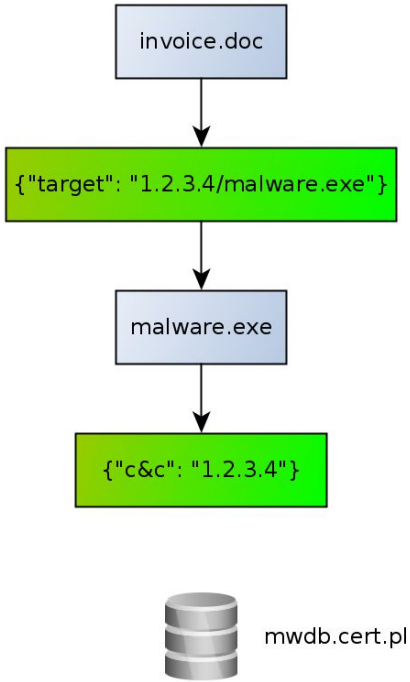
Ujście: mwdb.cert.pl

- **M**al**w**are **d**ata**b**ase
- Repozytorium dla naszych plików
- Razem z konfiguracja



Ujście: mwdb.cert.pl

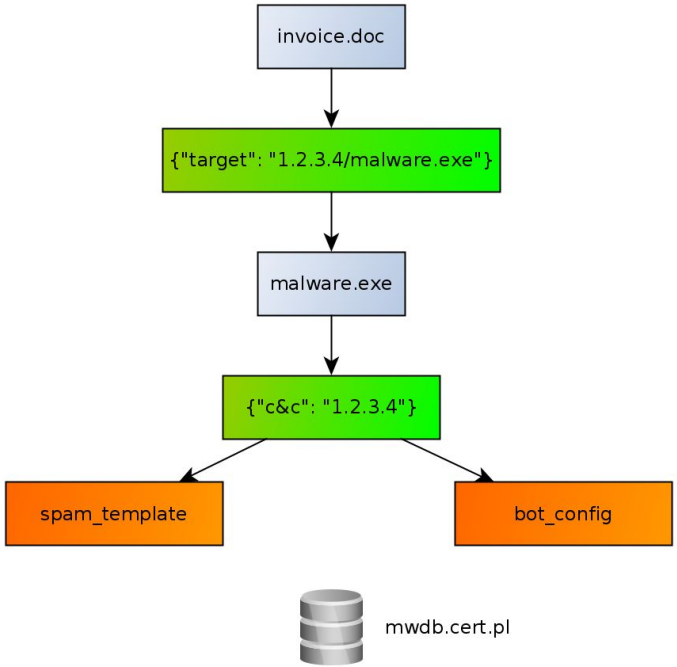
- **M**al**w**are **d**ata**b**ase
- Repozytorium dla naszych plików
- Razem z konfiguracja
- I relacjami rodzic-dziecko



CERT.PL >_

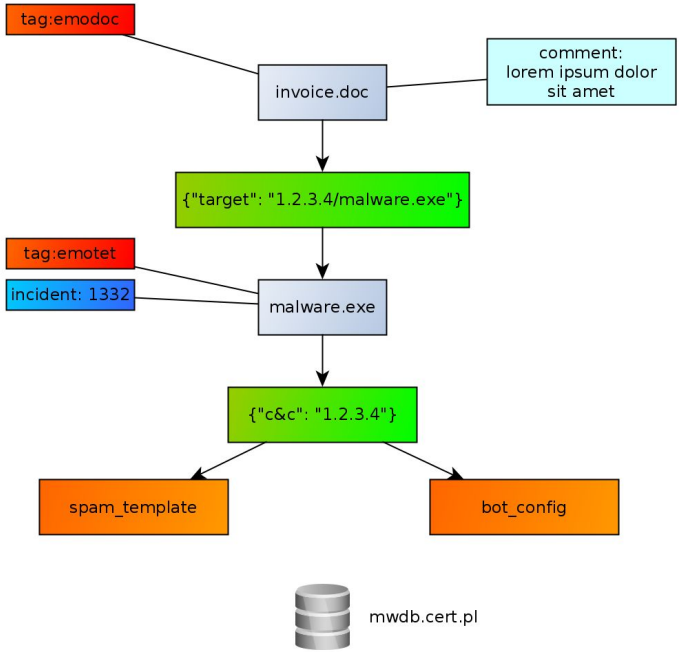
Ujście: mwdb.cert.pl

- **M**al**w**are **d**ata**b**ase
- Repozytorium dla naszych plików
- Razem z konfiguracja
- I relacjami rodzic-dziecko
- I dodatkowymi danymi



Ujście: mwdb.cert.pl

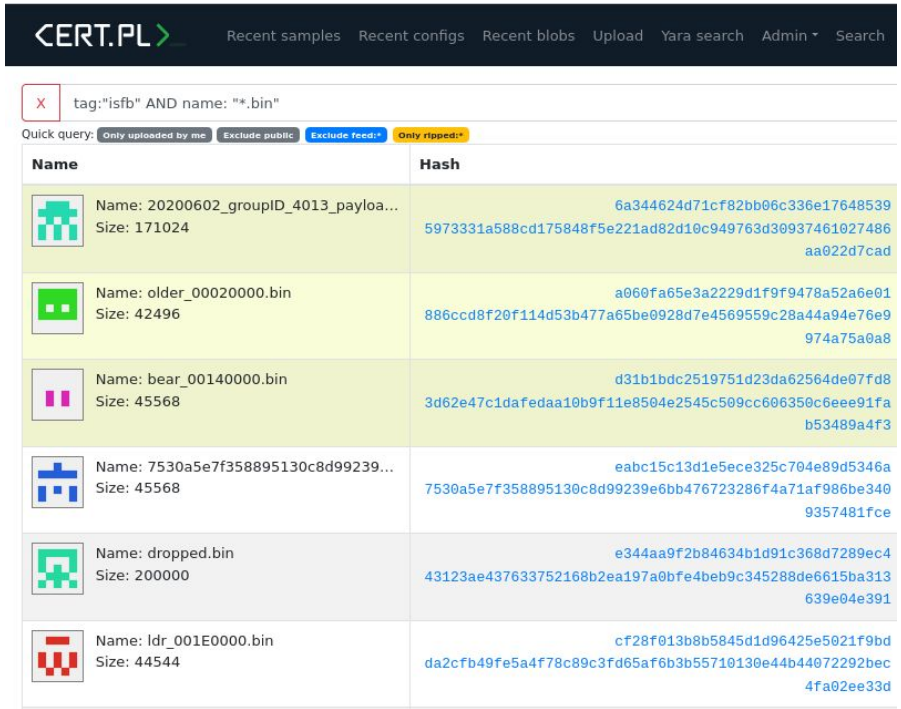
- **M**al**w**are **d**ata**b**ase
- Repozytorium dla naszych plików
- Razem z konfiguracja
- I relacjami rodzic-dziecko
- I dodatkowymi danymi
- I tagami, komentarzami, metadanymi



CERT.PL

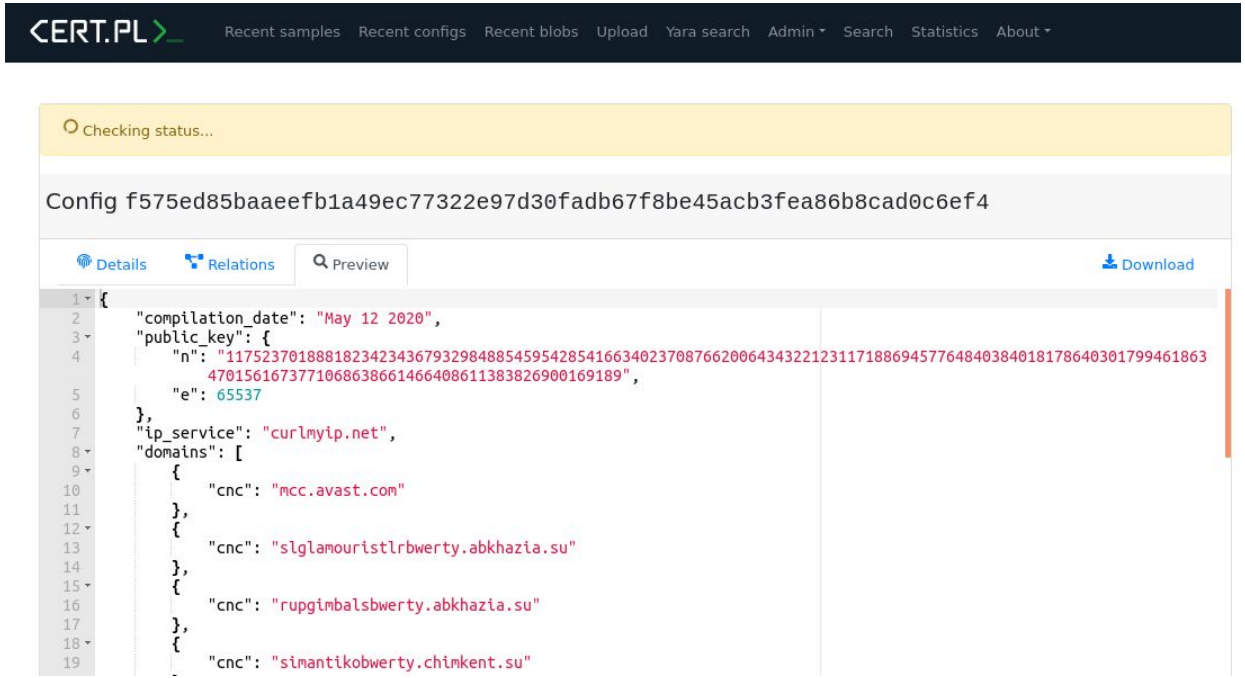
Ujście: mwdb.cert.pl

- **M**al**w**are **d**ata**b**ase
- Repozytorium dla naszych plików
- Razem z konfiguracja
- I relacjami rodzic-dziecko
- I dodatkowymi danymi
- I tagami, komentarzami, metadanymi
- I językiem zapytań (lucene)



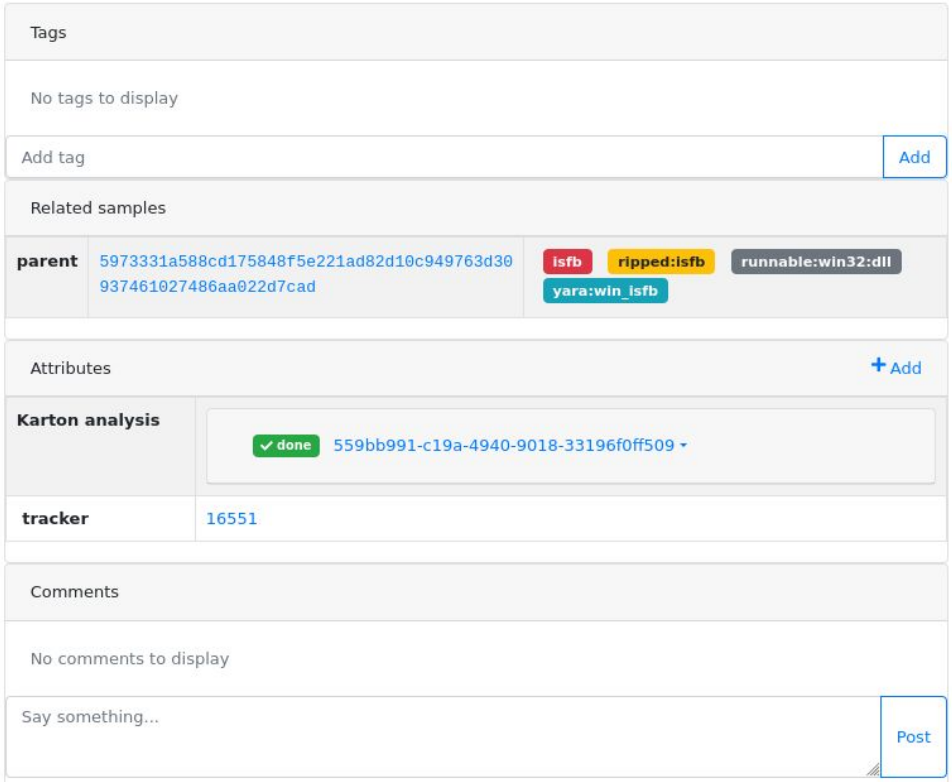
CERT.PL

Ujście: mwdb.cert.pl



CERT.PL

Ujście: mwdb.cert.pl



CERT.PL

Ujścia: systemy i systemiki

https://hole.cert.pl/domains/

https://injects.cert.pl/

MISP

Ujścia: ludzie

Podziękowania

CERT.PL >_

Podziękowania

[prawdopodobnie]

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

CERT.PL

Pytania?

Kontakt:

msm@cert.pl

info@cert.pl

jaroslaw.jedynak@cert.pl

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

CERT.PL