

jak zbierać złe dane 🖤 w dobrym celu 😇

Jarosław Jedynak

Secure EB
2020-06-16



secure
earlybird

Agenda

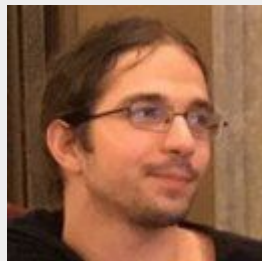
- Kim {jestem,jesteśmy}
- Temat prezentacji
- Nasze źródła danych
- I gdzie te dane wysyłamy



\$ whoami

Jarosław Jedynak

msm@cert.pl



\$ whoami

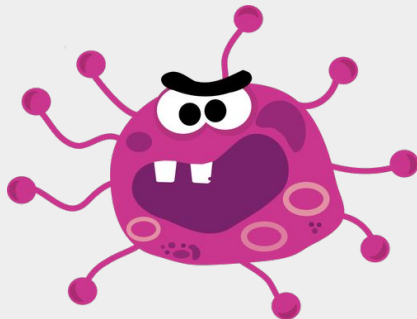
Jarosław Jedynak

msm@cert.pl



Analiza
złośliwego
oprogramowania

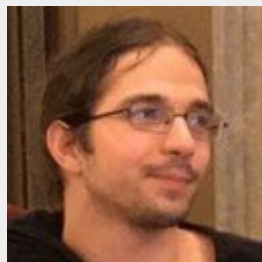
<CERT.PL>_



\$ whoami

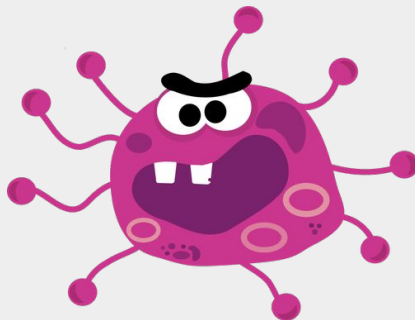
Jarosław Jedynak

msm@cert.pl



Analiza
złośliwego
oprogramowania

<CERT.PL>_



CTF @ p4.team
w "wolnym" czasie



<CERT.PL>_

\$ whoami

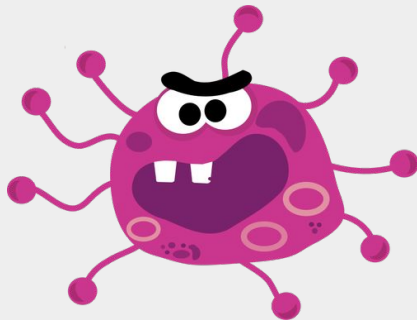
Jarosław Jedynak

msm@cert.pl



Analiza
złośliwego
oprogramowania

<CERT.PL>_



CTF @ p4.team
w "wolnym" czasie



Historycznie
inne zajęcia



<CERT.PL>_

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

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]

[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]

[redacted] szczegóły techniczne podatności będą musiały pozostać tajemnicą.



Michał Praszmo
CERT Polska

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? *****

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

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

Jarosław Jedynak
CERT Polska

Michał Praszmo
CERT Polska



Temat prezentacji

~~“jak zatrąć życie przestępcy”~~

jak zbierać dane

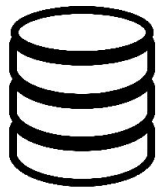


Dokąd zmierzamy

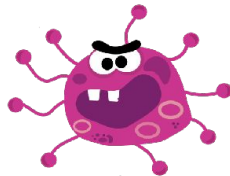


Dokąd zmierzamy

Publiczne zbiory danych
+ kręgi wymiany informacji



Złośliwe oprogramowanie
+ jego serwery



Działania operacyjne
+ wymiana informacji

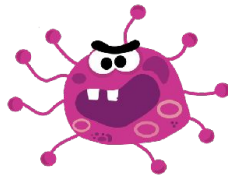


Dokąd zmierzamy

Publiczne zbiory danych
+ kręgi wymiany informacji



Złośliwe oprogramowanie
+ jego serwery



Działania operacyjne
+ wymiana informacji



n6.cert.pl



mwdb.cert.pl



kontakt z ludźmi

Źródła: Publiczne zbiory danych

Hasze złośliwego oprogramowania

Próbki złośliwego oprogramowania

Złośliwe URL

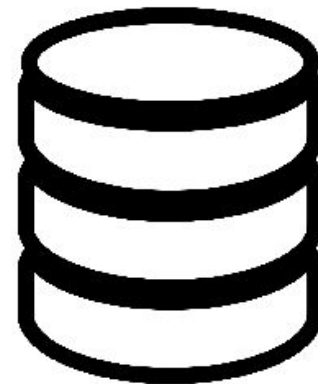
Złośliwe domeny

Czasami dodatkowe metadane



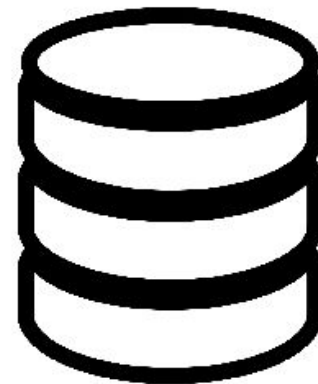
Źródła: Publiczne zbiory danych

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



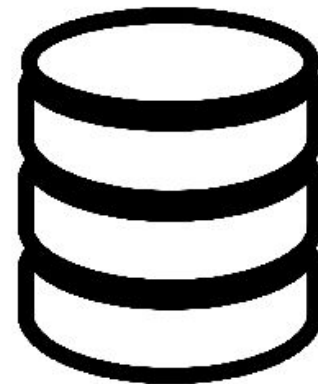
Źródła: Publiczne zbiory danych

- 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

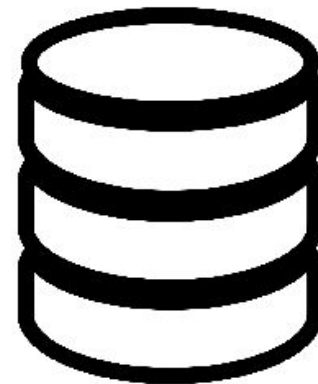
- URLhaus  (<https://urlhaus.abuse.ch/>)
- MalwareBazaar (<https://bazaar.abuse.ch/>)
- abuse.ch (<https://abuse.ch>)
- VxUnderground



URLhaus
by ABUSE|ch

MALWARE bazaar
by ABUSE|ch

ABUSE|ch



Źródła: Publiczne zbiory danych

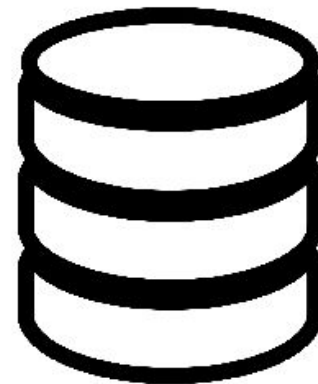
- URLhaus 💖 (<https://urlhaus.abuse.ch/>)
- MalwareBazaar (<https://bazaar.abuse.ch/>)
- abuse.ch (<https://abuse.ch>)
- VxUnderground
- VirusShare



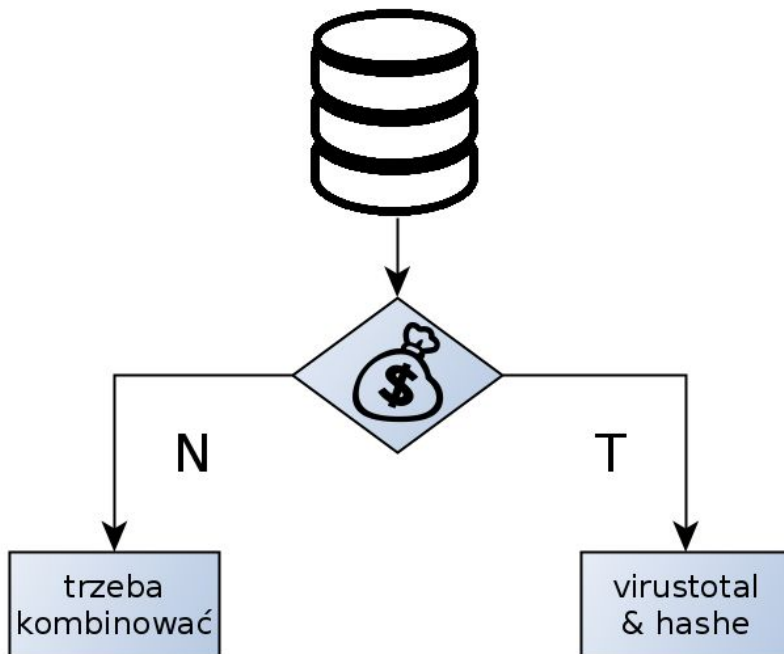
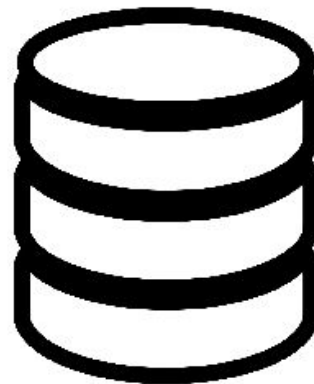
URLhaus
by ABUSE|ch

MALWARE bazaar
by ABUSE|ch

ABUSE|ch



Źródła: Publiczne zbiory danych



(dla analityków, nie blacklist)

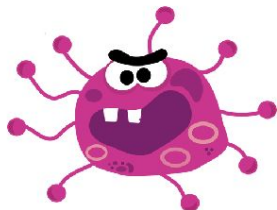
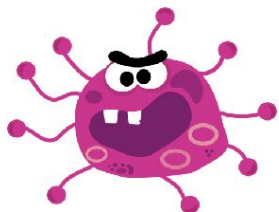
Źródła: Publiczne zbiory danych



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

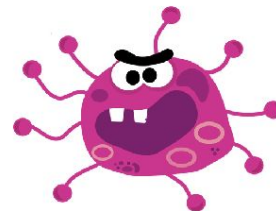
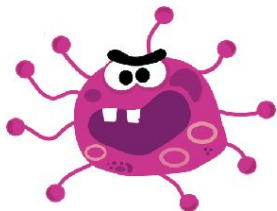
[Download CSV \(online URLs only\)](#)

Źródła: Publiczne zbiory danych



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

Do (only online URLs only)



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>)



Źródła: Złośliwe oprogramowanie

Więcej próbek złośliwego oprogramowania

URLe i domeny serwerów C2

Klucze do komunikacji

Identyfikatory kampanii

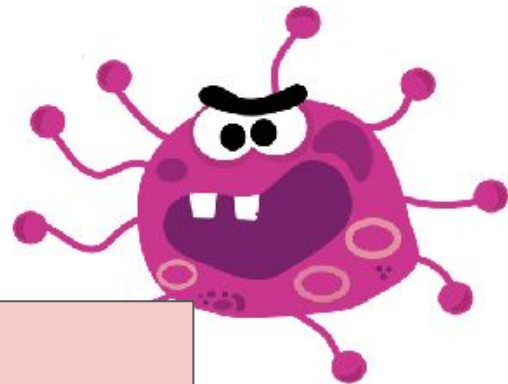
Konfiguracja kampanii

Szablony wiadomości spamowych

IP innych peerów w botnecie

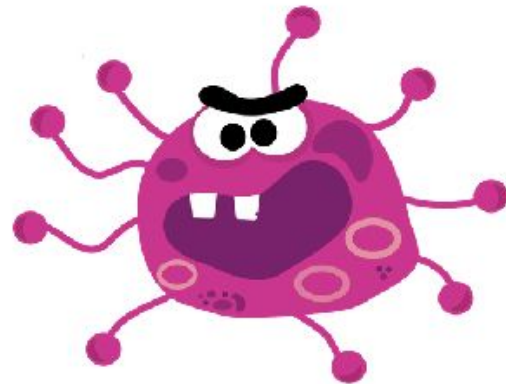
Pliki z żądaniem okupu

Zaszyte hardkodowane hasła



Źródła: Złośliwe oprogramowanie

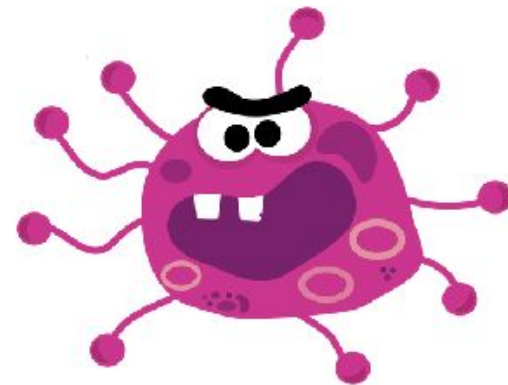
Czyli “o tym już chyba była prezentacja”



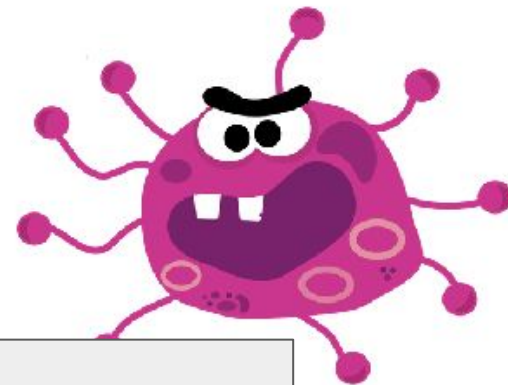
Źródła: Złośliwe oprogramowanie

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"

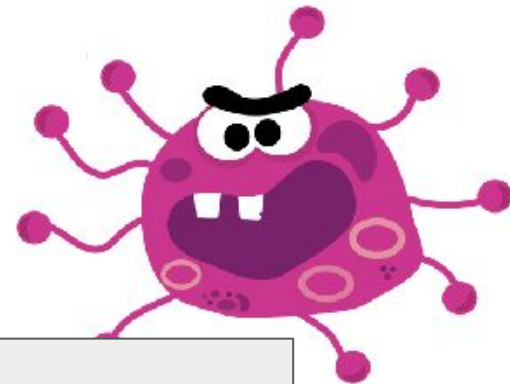
Łukasz Siewierski
"(Mostly) Polish threat landscape: not only VBKlip"

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



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

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”

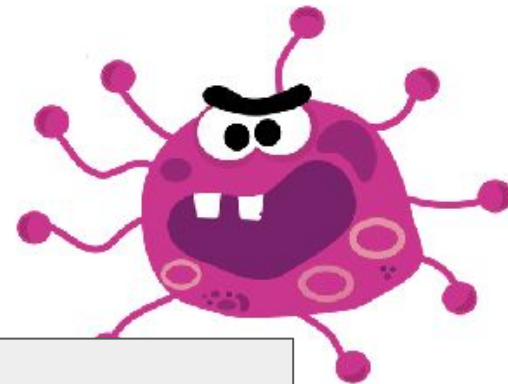
Maciej Kotowicz
“ZeuS meets VM, story so far”

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 Jedynek, Paweł Srokosz.
“Use your enemies: tracking botnets with bots”

Maciej Kotowicz
“ZeuS meets VM, story so far”

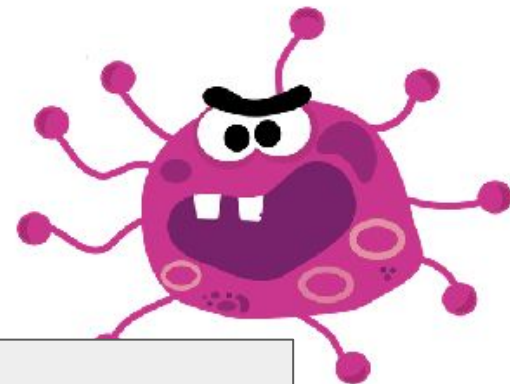
Maciej Kotowicz
“Malware Calling”



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 Jedynek, Maciej Kotowicz
"Nymaim, the untold story"

Jarosław Jedynek, Paweł Srokosz.
"Nymaim: tracking botnets with bots"

Jarosław Jedynek, Maciej Kotowicz
"Peering into spambotnets"

Michał Leszczyński, Krzysztof Stopczyński
"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"

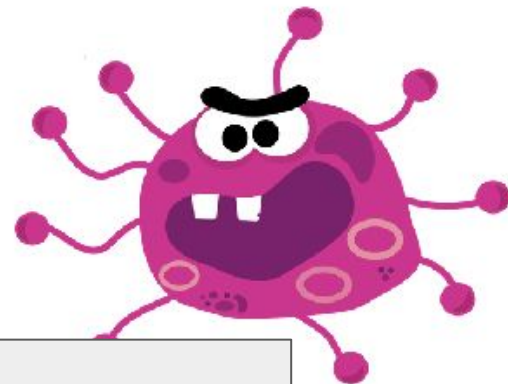
Źródła: Złośliwe oprogramowanie



Czyli "o ty

Tomasz Bukowski
"ZitMo - case study"

tacja"



Maciej Kotowicz
"ISFB, Still Live and Kicking"

Łukasz Siewierski
"(Mostly) Polish threat land

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 Leszczynski, Krzysztof Stopczyński
"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

Paweł Krześniak

"Wykrywanie podejrzanych domen internetowych
poprzez pasywną analizę ruchu DNS"

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

Piotr Kijewski
"Platforma n6"

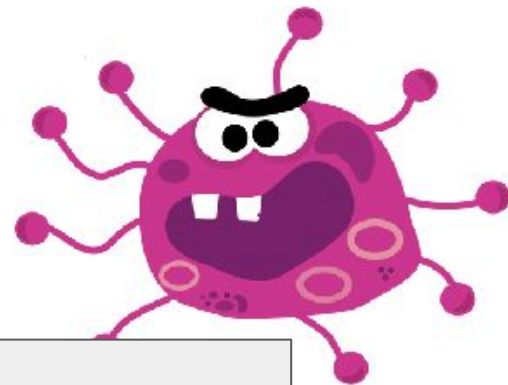
Źródła: Złośliwe oprogramowanie

secure
2011

Czyli "o ty

Tomasz Bukowski
"ZitMo - case study" tacja"

virus
BULLETIN



Maciej Kotowicz
"ISFB, Still Live and Kicking"

Łukasz Siewierski
"(Mostly) Polish threat land

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 Leszczynski, Krzysztof Stopczyński
"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

Paweł Krześniak

"Wykrywanie podejrzanych domen internetowych
poprzez pasywną analizę ruchu DNS"

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

Piotr Kijewski
"Platforma n6"

Źródła: Złośliwe oprogramowanie

secure
2011

Czyli "o ty

Tomasz Bukowski
"ZitMo - case study"

virus

secure
2012

Radosław Żuber "Ataki na systemy bankowości elektronicznej"

Maciej Kotowicz
"ISFB, Still Live and Kicking"

Łukasz Siewierski
"(Mostly) Polish threat land

Tomasz Sałaciński
"Techniki anti-reversing w botach SpyEye"

Paweł Jacewicz, Łukasz Juszczyk
"Anatomia złośliwego PDFa"

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

Jarosław Jedynak, Maciej Kotowicz
"Peering into spambotnets"

Michał Leszczynski, Krzysztof Stopczyński

Paweł Pawliński
"Honey Spider Network 2.0"

Łukasz Juszczyk "Wykrywanie oraz analiza ataków na sieci komputerowe"

ring and extraction system"

sz Bukowski, Tomasz Sałaciński

Piotr Białczak "Leaving no Stone Unturned - in

"Analiza Spy

Radosław Żuber "Co w sieci piszczy..."

ware Actors in

Paweł Krześniak

"Wykrywanie podejrzanych domen internetowych poprzez pasywną analizę ruchu DNS"

Piotr Kijewski
"Platforma n6"

Źródła: Złośliwe oprogramowanie

secure
2012

secure
2011

Czyli "o ty

Tomasz B

"ZitMo - Case study

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

Radosław Zuber "Ataki na systemy bankowości elektronicznej"

Maciej Kotowicz
"ISFB, Still Live &

Piotr Kijewski
"CERT Polska vs botnety"

Łukasz Siewierski
"ish threat land

Tomasz Sałaciński
"Techniki anti-reversing w botach SpyEye"

secure
2013

Paweł Jacewicz, Łukasz Juszczyk
"Anatomia złośliwego PDFa"

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

Jarosław Jedynak, Maciej Kotowicz
"Peering into spambotnets"

Michał Leszczynski, Krzysztof Stopczyński

Paweł Pawliński
"er Network 2.0"

Łukasz Juszczyk "Wykrywanie oraz analiza ataków na sieci komputerowe"

ring and extr
Paweł Pawliński
"n6: otwarta wymiana danych"

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

secure
2011

Czyli "o ty

Tomasz B...
"ZitMo - Ca

Tomar

secure
2012

"Intruz w sieci. Wykrywanie
korporacyjnych

na systemy
ej"

secure
2013

Maciej Kotowicz
"ISFB, Still Live &

Piotr Kijewski
"CERT Po

Jarosław Jedynak, Maciej K

Paweł Jacewicz, Łukasz Jus
"Anatomia złośliwego PDFa

Michał Leszczyński

aciński

anti-reversing w botach SpyEye"

Jarosław Jedynak, Maciej Kotowicz
ering into spambotnets"

Paweł Pawliński

er Network 2.0"

Łukasz Juszczak "Wykrywanie o
analiza ataków na sieci komputerow

iania danych"

Tomasz Bukowski, Łukasz Siewierski
"Wyszukiwanie i identyfikacja śladów info

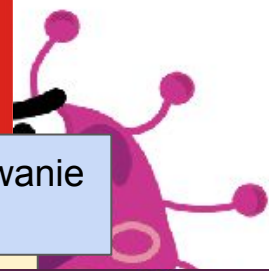
nowaniem"

piszczy..."

ware Actors in

"Wykrywanie podejrzanych domen internetowych
poprzez pasywną analizę ruchu DNS"

Piotr Kijewski
"Platforma n6"

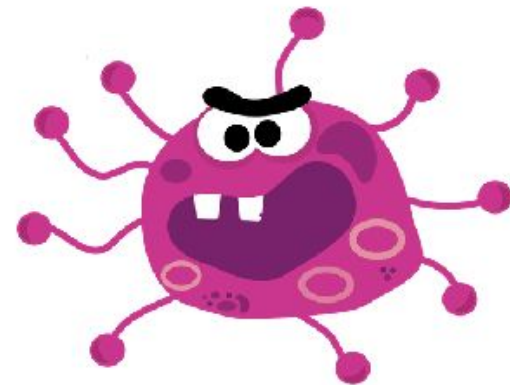


Źródła: Złośliwe oprogramowanie

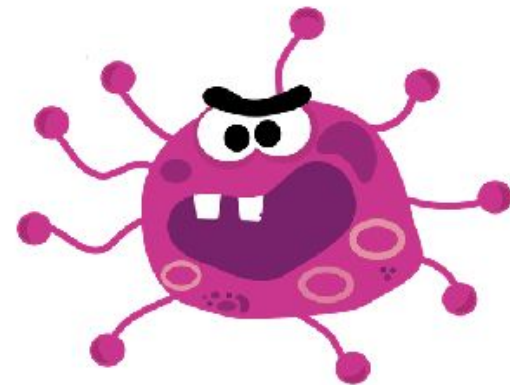
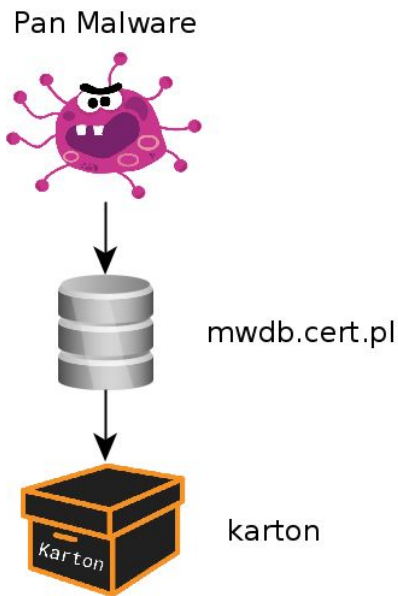
Pan Malware



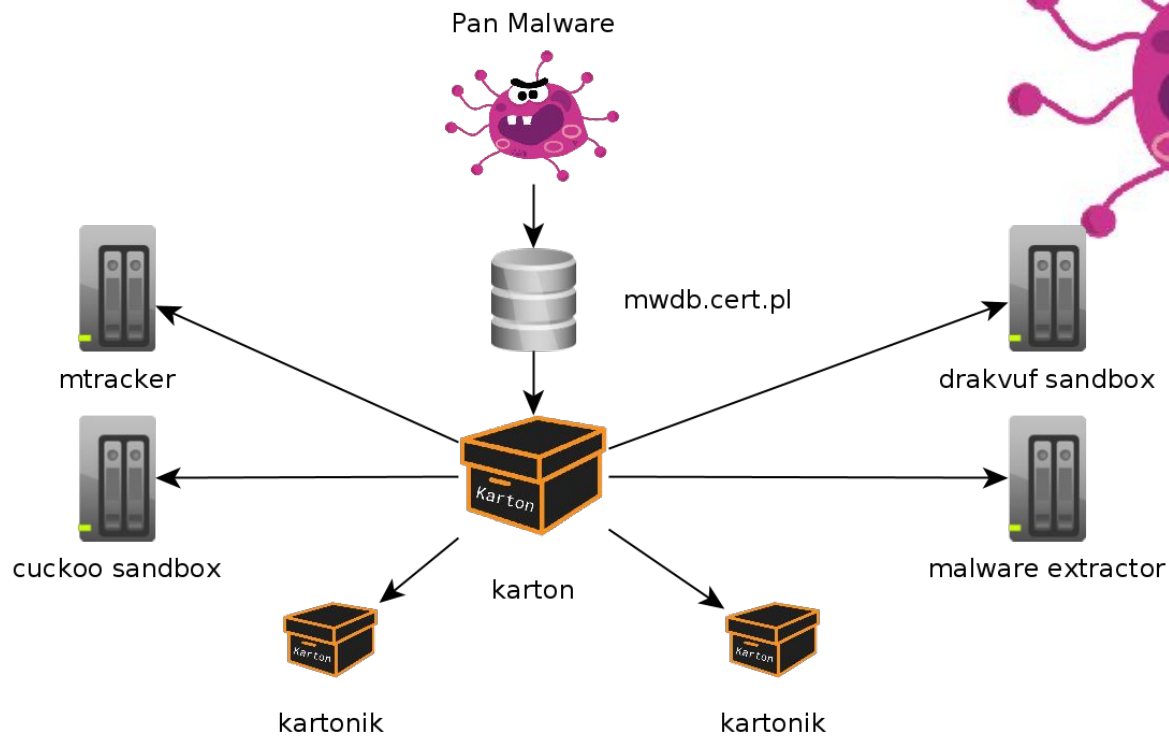
mwdb.cert.pl



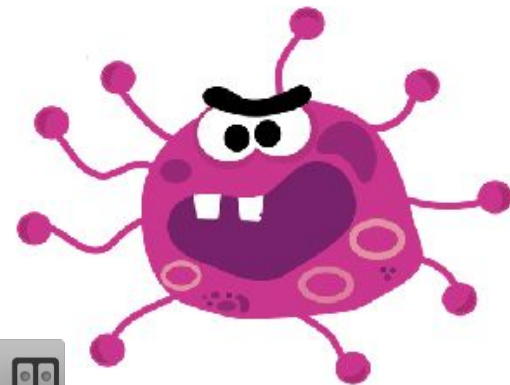
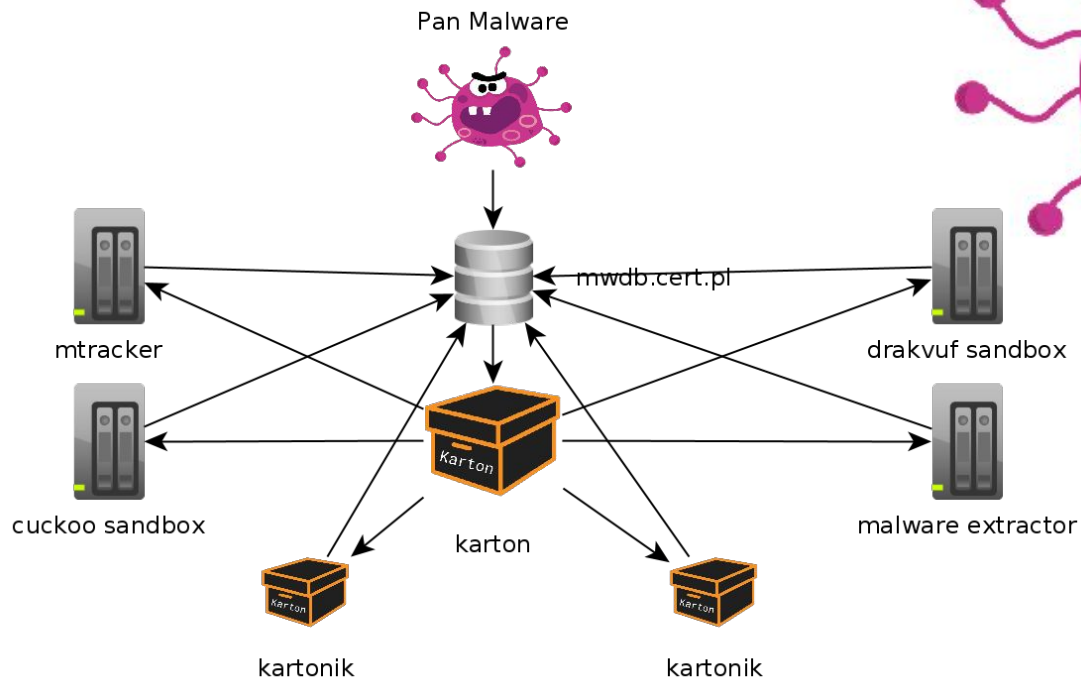
Źródła: Złośliwe oprogramowanie



Źródła: Złośliwe oprogramowanie



Źródła: Złośliwe oprogramowanie



Źródła: Złośliwe oprogramowanie

```
from ripper import Extractor
```

<https://malduck.readthedocs.io>

```
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):
```

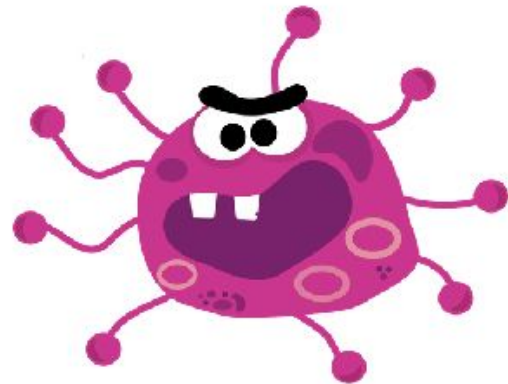
```
        return {'login_key': p.asciiz(hit)}
```

```
    hit = p.uint32v(addr + 5)
```

```
    print(hex(hit))
```

```
    if p.is_addr(hit):
```

```
        return {'login_key': p.asciiz(hit)}
```



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 Zatrucć 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



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

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



Źródła: Dane “zebrane ręcznie”

Samodzielnie albo z pomocą innych



Zgłaszanie podejrzanych stron

Każdy może zgłosić stronę, która może wyludzać 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>

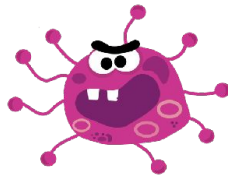
Pliki są aktualizowane co 5 minut. Pełna specyfikacja naszego API [dostępna jest tutaj](#).

Dokąd zmierzamy

Publiczne zbiory danych
+ kręgi wymiany informacji



Złośliwe oprogramowanie
+ jego serwery



Działania operacyjne
+ wymiana informacji



n6.cert.pl



mwdb.cert.pl



kontakt z ludźmi

Dygresja językowa: “sink”?



Images for sink



kitchen



stainless steel



modern



bowl

Source -> Sink
Źródło -> ???



→ More images for sink

Report images

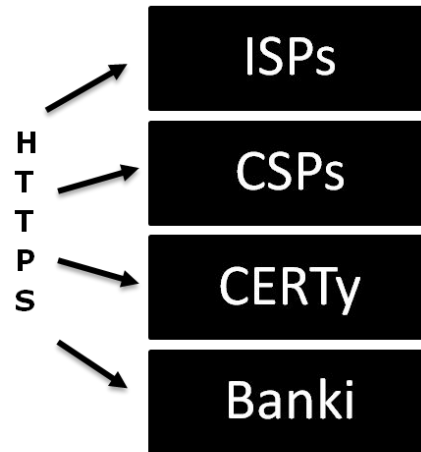
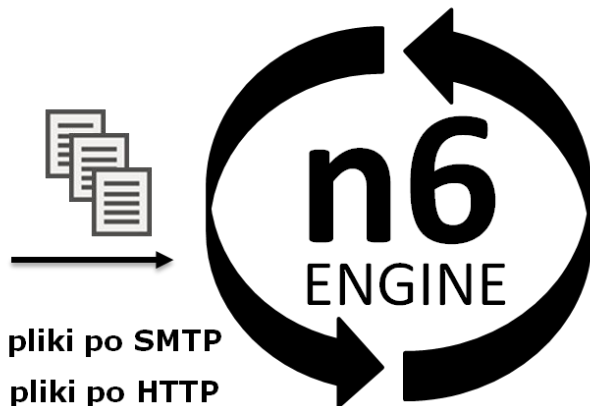
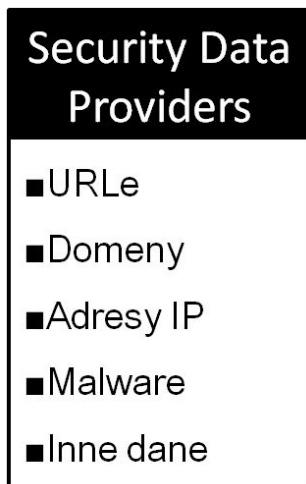
Ujście: n6

Dostępne dla: administratorów sieci, CERTów.

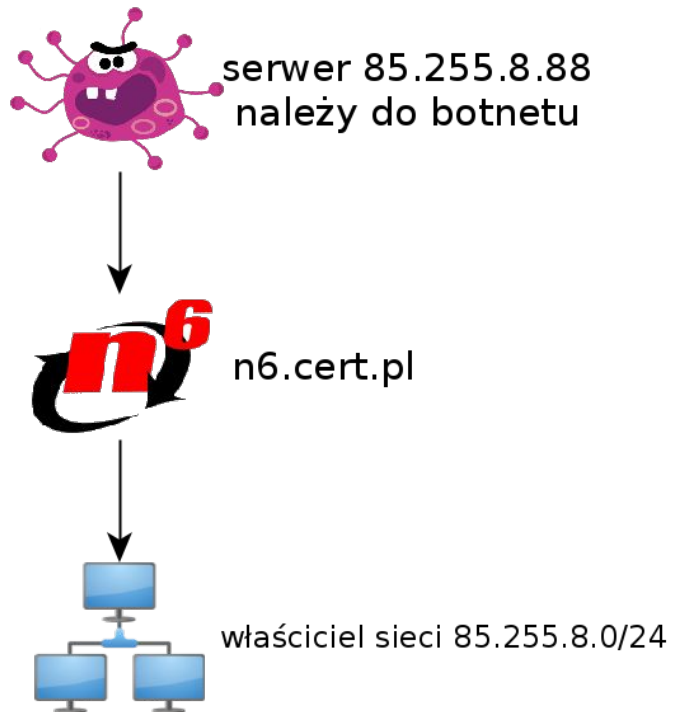
Dane: informacje o incydentach.



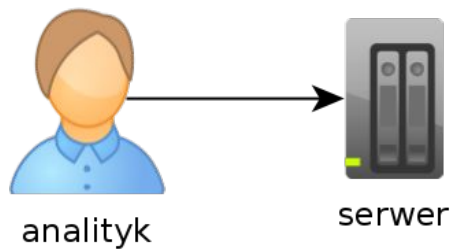
Ujście: n6



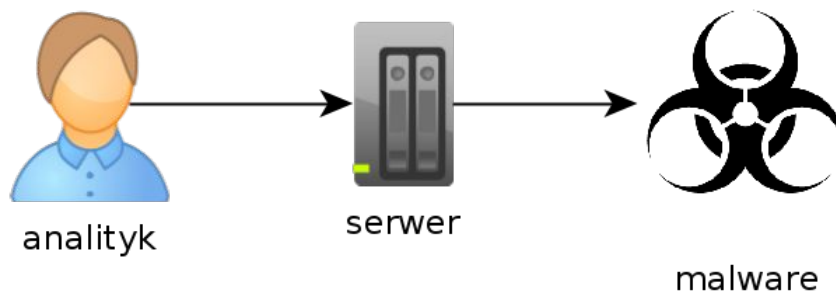
Ujście: n6



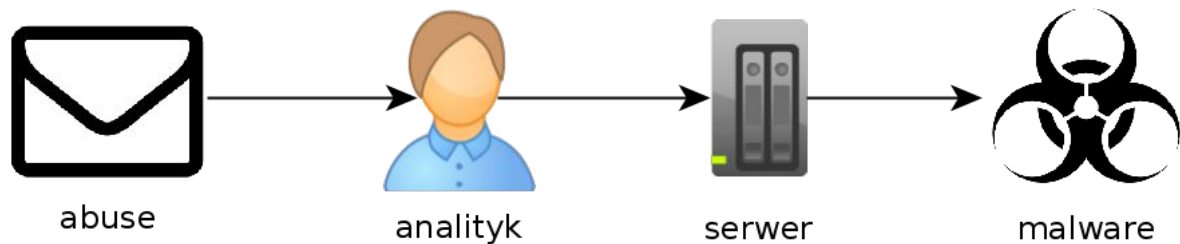
Dygresja: Przepływ danych



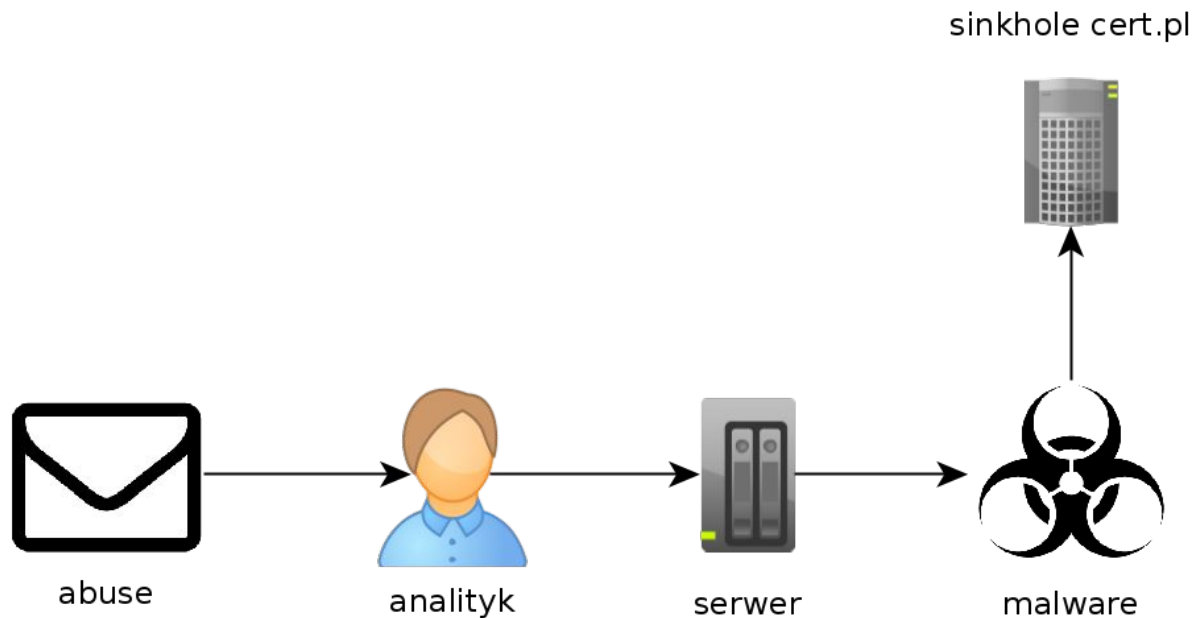
Dygresja: Przepływ danych



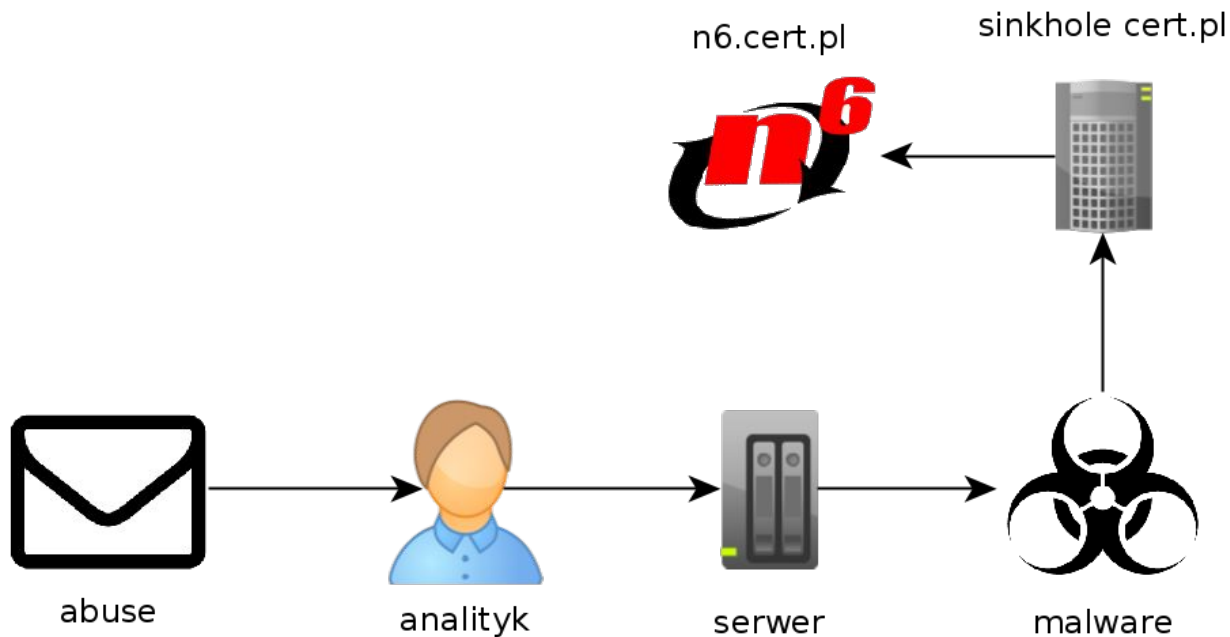
Dygresja: Przepływ danych



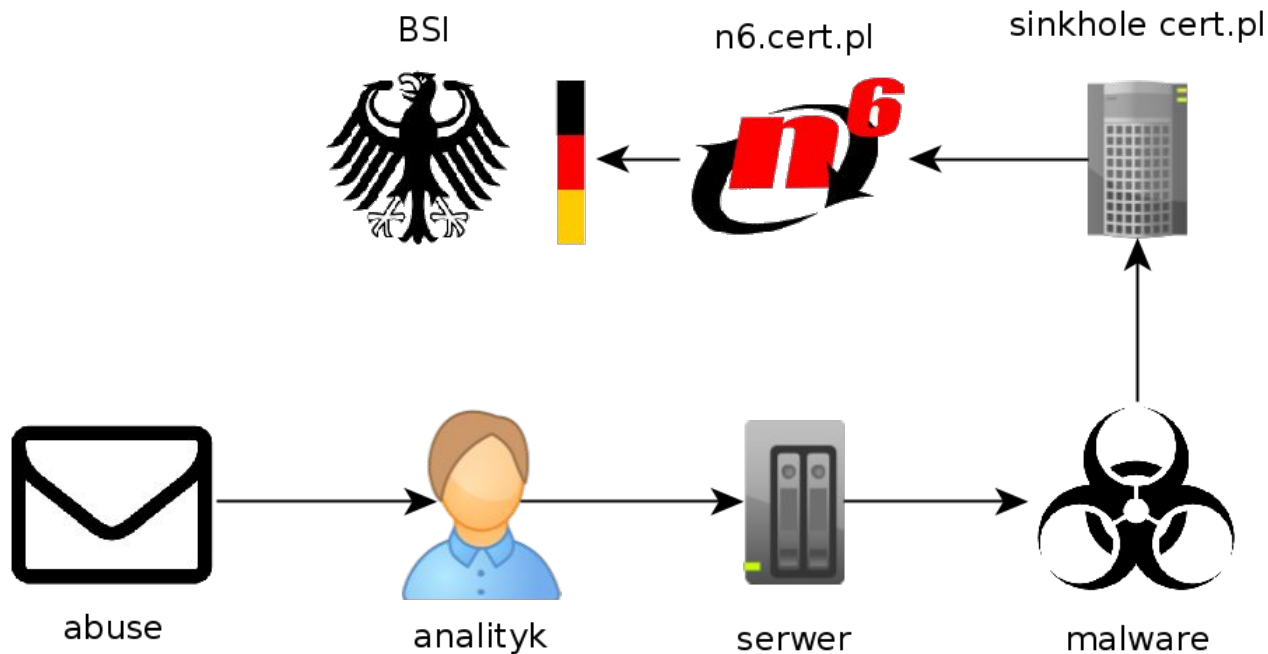
Dygresja: Przepływ danych



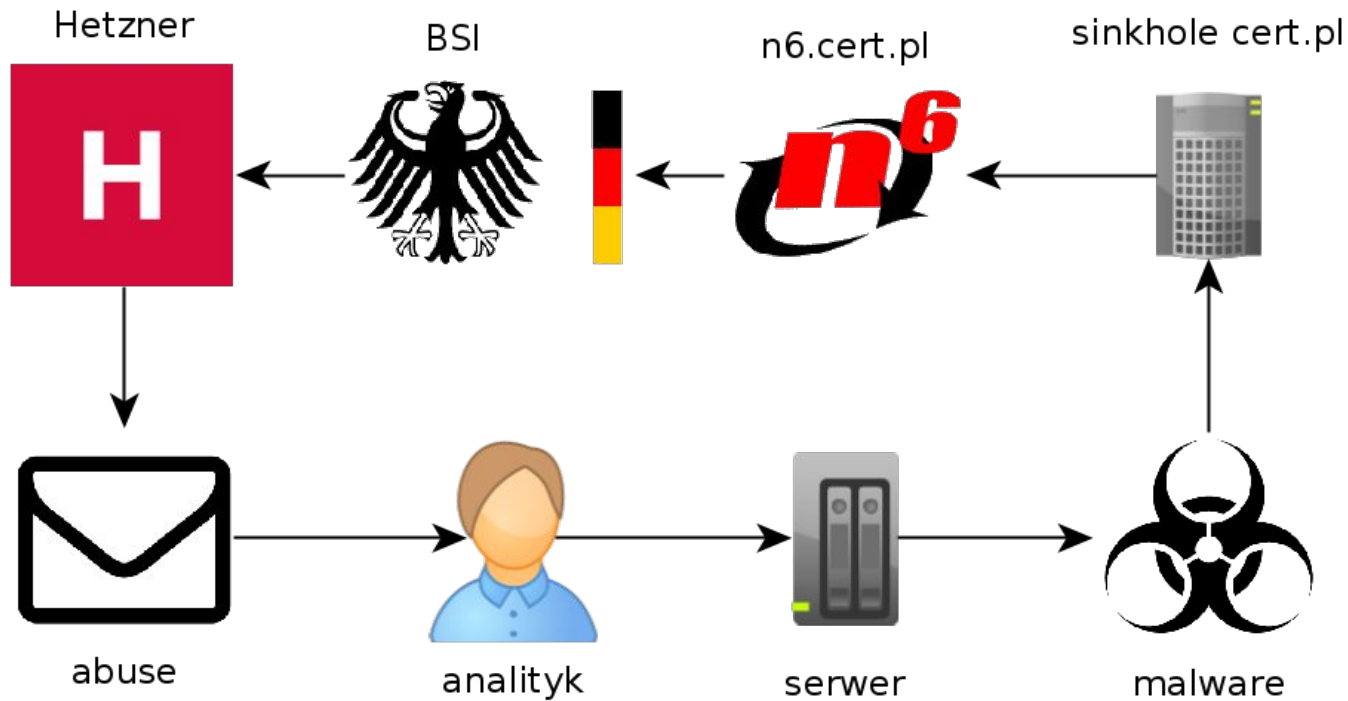
Dygresja: Przepływ danych



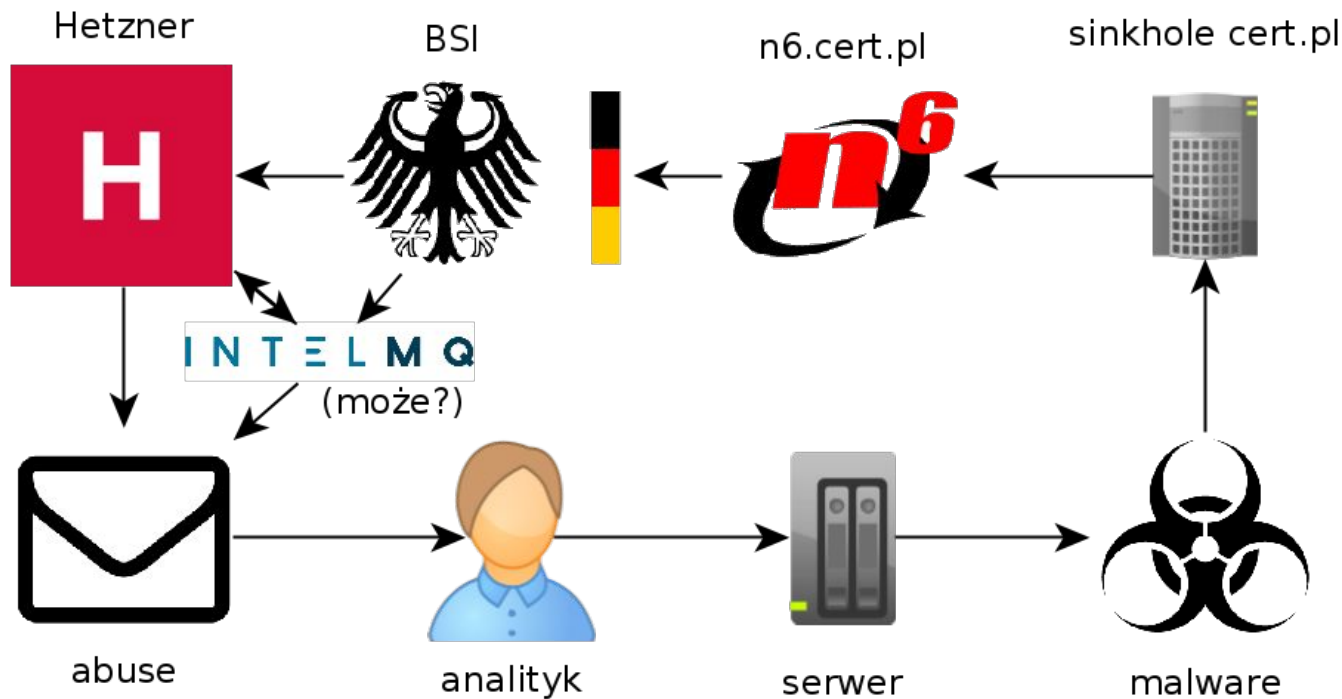
Dygresja: Przepływ danych



Dygresja: Przepływ danych



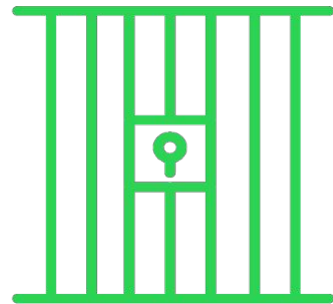
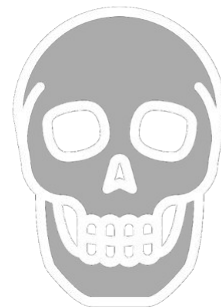
Dygresja: Przepływ danych



Ujście: mwdb

Dostępne dla: analityków malware

Dane: informacje o próbkach.











Ujście: mwdb.cert.pl

CERT.PL > Recent samples Recent configs Recent blobs Upload Yara search Admin* Search Statistics About*

Logged as: msm Profile Logout

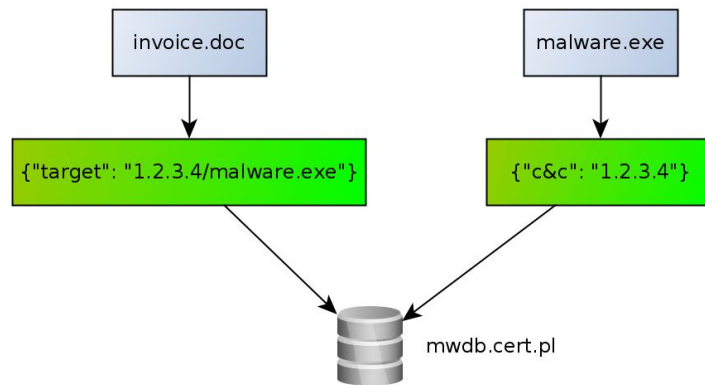
X Search (Lucene query or hash)... Search ?

Quick query: Only optimized by ms Exclude public Exclude feeds Only featured

Name	Hash	File type	Tags	Creation Time
 Name: 339410_0014297256_JED_00139... Size: 10834	194e4196875b4d77f9e6527c13533695 5abf6b135aebca306efaf019797b955b a8558d55eeecfc671b13c87f9c1a22f	Rich Text Format data, unknown version	document:win32:rtf feed:spam	Mon, 01 Jun 2020 18:53:01 GMT
 Name: Host_WTDRIUh117.bin Size: 151616	3cf021e4d17c9e379aec9b9965b31da ec92fa63986e7c991af4c8f7b7b382f d6386867be395a42ebe3b89de4e728c9	data	feed:urlhaus urlhaus:encrypted urlhaus:guloader	Mon, 01 Jun 2020 18:42:05 GMT
 Name: Host_SsDkeblSIV45.bin Size: 164416	d4640e760e91173c9e9ce00291e54241 843408c230f7688f2044e39af99f16e6 5c3028a51c2c220c24820d408211afb2	data	feed:urlhaus urlhaus:encrypted urlhaus:guloader	Mon, 01 Jun 2020 18:41:41 GMT
 Name: uc Size: 40709	07ecfcec4c3948ad48e2f0f35f3d7d59 e253e5b92ce8575372cad8e19a451b726 e0fcfc4a8f45cf658b21928e523e9bb6	PE32 executable (GUI) Intel 80386 Mono/.Net as...	guloader_drop runnable:win32:exe	Mon, 01 Jun 2020 18:29:15 GMT
 Name: 80000_40aefaba17ad2e8f Size: 184320	195c44fd67661c7b197aae29c7ab80 46aefaba17ad2e8f170a93d686136a73 bf7b051e67f78b1c9f56b120a0db2747	data	dump:win32:exe formbook	Mon, 01 Jun 2020 18:22:33 GMT
 Name: silk.dll Size: 662528	8376547617b35cd1c02de20c690c8bfe d896054df1e0325da674b72335ae3be6 1261aeea9b4cd93edd7b29aa63d059a	PE32 executable (DLL) (GUI) Intel 80386, for MS ...	ripped:zloader runnable:win32:dll yara:win_zloader	Mon, 01 Jun 2020 18:18:34 GMT
 Name: vbc.exe Size: 326656	8517c99744b43646ba22f7452a140997 b39a215a209c492ec94f6da67af44090 8c8a8c2239a37bbc1204538341823d88	PE32 executable (GUI) Intel 80386, for MS Windo...	st:formbook feed:urlhaus ripped:formbook runnable:win32:exe urlhaus:exe yara:win_formbook	Mon, 01 Jun 2020 18:12:21 GMT
 Name: 7fc83d10813a8dfc12ebad48bd0... Size: 217088	696c37a4ca7c9ab39eb91b8e27562a0d 7fc83d10813a8dfc12ebad48bd0928ed aabb48c40be56bd78fd412dae11b613	PE32+ executable (DLL) (GUI) x86-64, for MS Wi...	runnable:win64:dll	Mon, 01 Jun 2020 18:02:55 GMT

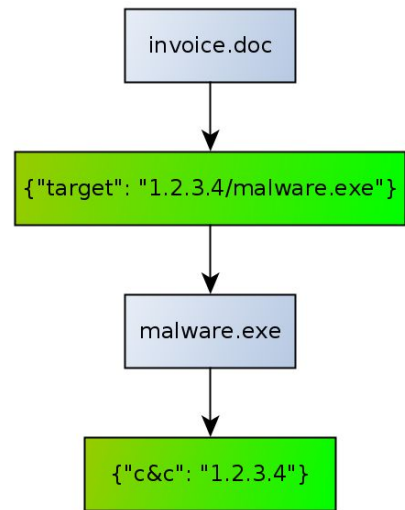
Ujście: mwdb.cert.pl

- Malware database
- Repozytorium dla naszych plików
- Razem z konfiguracją



Ujście: mwdb.cert.pl

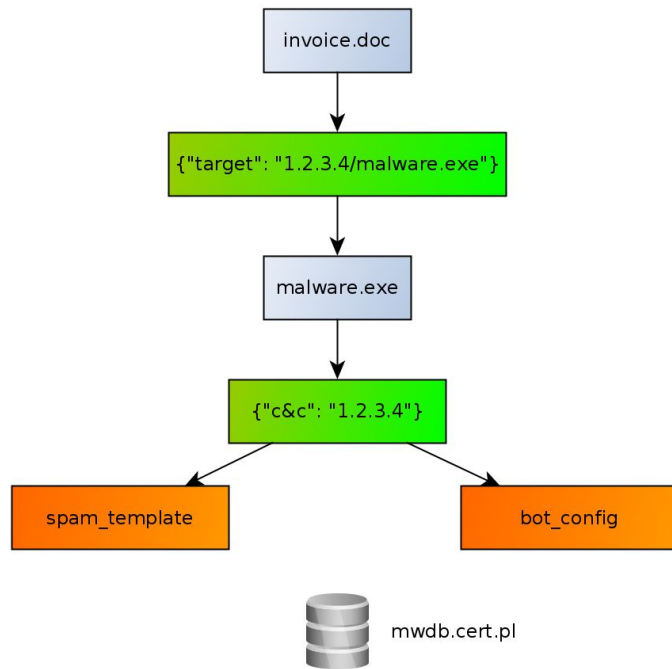
- Malware database
- Repozytorium dla naszych plików
- Razem z konfiguracją
- I relacjami rodzic-dziecko



mwdb.cert.pl

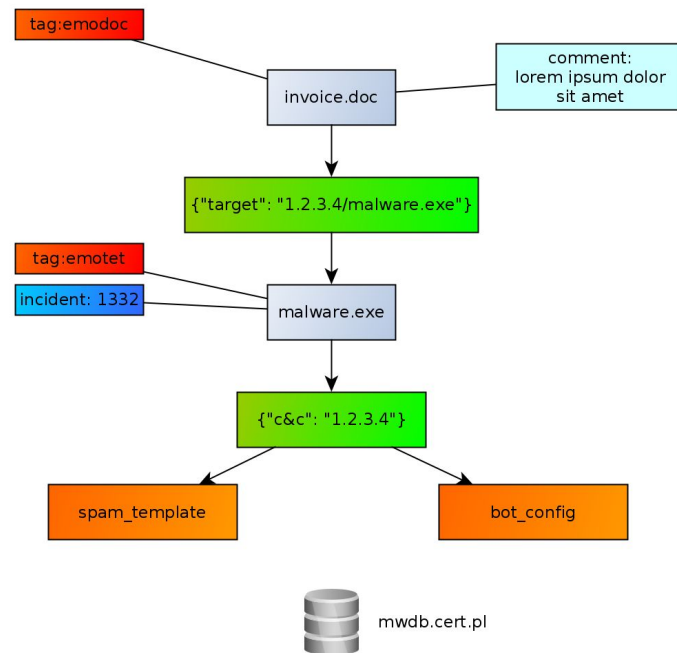
Ujście: mwdb.cert.pl

- Malware database
- Repozytorium dla naszych plików
- Razem z konfiguracją
- I relacjami rodzic-dziecko
- I dodatkowymi danymi



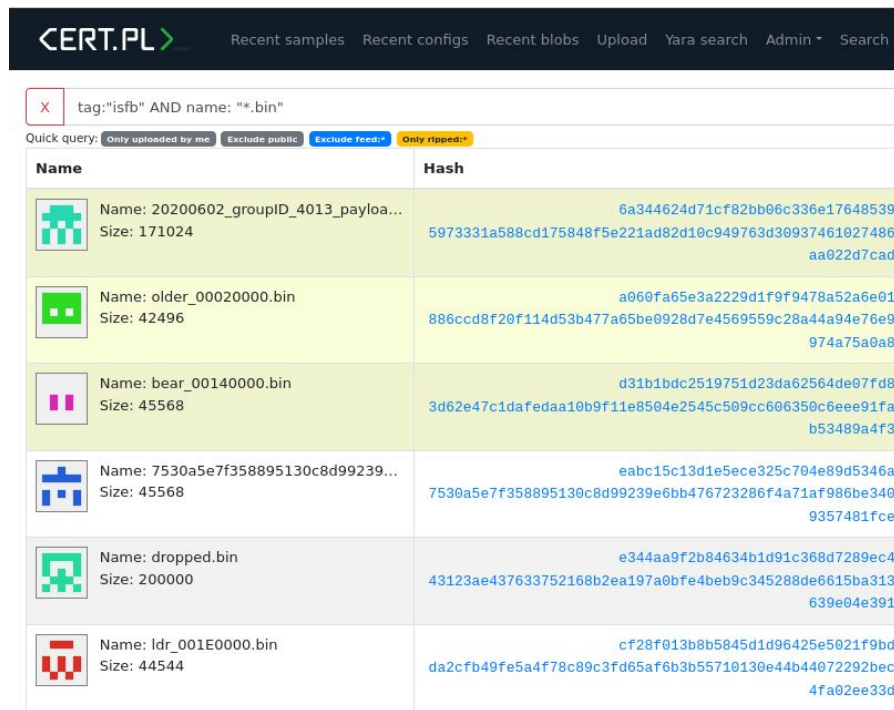
Ujście: mwdb.cert.pl

- Malware database
- Repozytorium dla naszych plików
- Razem z konfiguracją
- I relacjami rodzic-dziecko
- I dodatkowymi danymi
- I tagami, komentarzami, metadanymi









Ujście: mwdb.cert.pl

- Malware database
- Repozytorium dla naszych plików
- Razem z konfiguracja
- I relacjami rodzic-dziecko
- I dodatkowymi danymi
- I tagami, komentarzami, metadanymi
- I językiem zapytań (lucene)



The screenshot shows the mwdb.cert.pl web interface. At the top, there is a navigation bar with the logo and links for 'Recent samples', 'Recent configs', 'Recent blobs', 'Upload', 'Yara search', and 'Admin'. Below the navigation bar, a search query is entered: 'tag:"isfb" AND name: "*.bin"'. The search results are displayed in a table with two columns: 'Name' and 'Hash'. Each row includes a small icon representing the sample type, the sample name and size, and the corresponding hash value.

Name	Hash
 Name: 20200602_groupID_4013_payloa... Size: 171024	6a344624d71cf82bb06c336e17648539 5973331a588cd175848f5e221ad82d10c949763d30937461027486 aa022d7cad
 Name: older_00020000.bin Size: 42496	a060fa65e3a2229d1f9f9478a52a6e01 886ccd8f20f114d53b477a65be0928d7e4569559c28a44a94e76e9 974a75a0a8
 Name: bear_00140000.bin Size: 45568	d31b1bdc2519751d23da62564de07fd8 3d62e47c1dafedaa10b9f11e8504e2545c509cc606350c6eee91fa b53489a4f3
 Name: 7530a5e7f358895130c8d99239... Size: 45568	eabc15c13d1e5ece325c704e89d5346a 7530a5e7f358895130c8d99239e6bb476723286f4a71af986be340 9357481fce
 Name: dropped.bin Size: 200000	e344aa9f2b84634b1d91c368d7289ec4 43123ae437633752168b2ea197a0bf44eb9c345288de6615ba313 639e04e391
 Name: ldr_001E0000.bin Size: 44544	cf28f013b8b5845d1d96425e5021f9bd da2cfb49fe5a4f78c89c3fd65af6b3b55710130e44b44072292bec 4fa02ee33d

Ujście: mwdb.cert.pl

CERT.PL > Recent samples Recent configs Recent blobs Upload Yara search Admin Search Statistics About

Checking status...

Config f575ed85baaeefb1a49ec77322e97d30fad67f8be45acb3fea86b8cad0c6ef4

Details Relations Preview Download

```
1 {
2   "compilation_date": "May 12 2020",
3   "public_key": {
4     "n": "1175237018881823423436793298488545954285416634023708766200643432212311718869457764840384018178640301799461863
      4701561673771068638661466408611383826900169189",
5     "e": 65537
6   },
7   "ip_service": "curlmyip.net",
8   "domains": [
9     {
10      "cnc": "mcc.avast.com"
11    },
12    {
13      "cnc": "slglamouristlrbwerty.abkhazia.su"
14    },
15    {
16      "cnc": "ruggimbalsbwerty.abkhazia.su"
17    },
18    {
19      "cnc": "sinantikobwerty.chimkent.su"
20    }
21  ]
22 }
```

Ujście: mwdb.cert.pl

Tags	
No tags to display	
Add tag	Add
Related samples	
parent	5973331a588cd175848f5e221ad82d10c949763d30937461027486aa022d7cad isfb ripped:isfb runnable:win32:dll yara:win_isfb
Attributes + Add	
Karton analysis	✓ done 559bb991-c19a-4940-9018-33196f0ff509 ▾
tracker	16551
Comments	
No comments to display	
Say something...	Post

Ujścia: systemy i systemiki

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

<https://injects.cert.pl/>

MISP

Ujścia: ludzie



Podziękowania



Podziękowania



[prawdopodobnie]

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

Pytania?

Kontakt:

msm@cert.pl

jaroslaw.jedynak@cert.pl

info@cert.pl



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

