XXIII MIĘDZYNARODOWY KONGRES OTWARTEGO SYSTEMU OCHRONY ZDROWIA OSOZ

REFERAT:

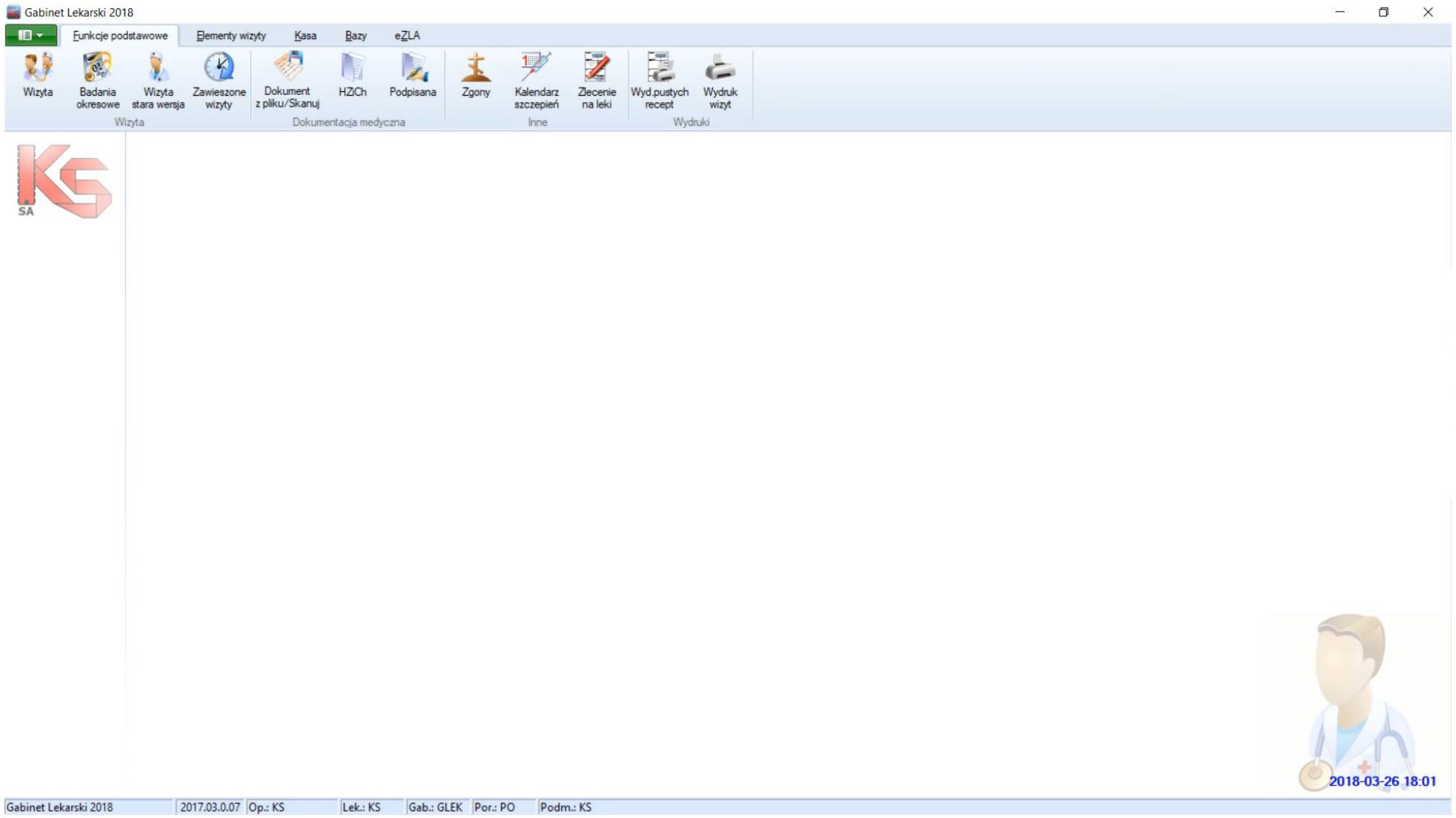
Case Study: Atak typu ransomware.

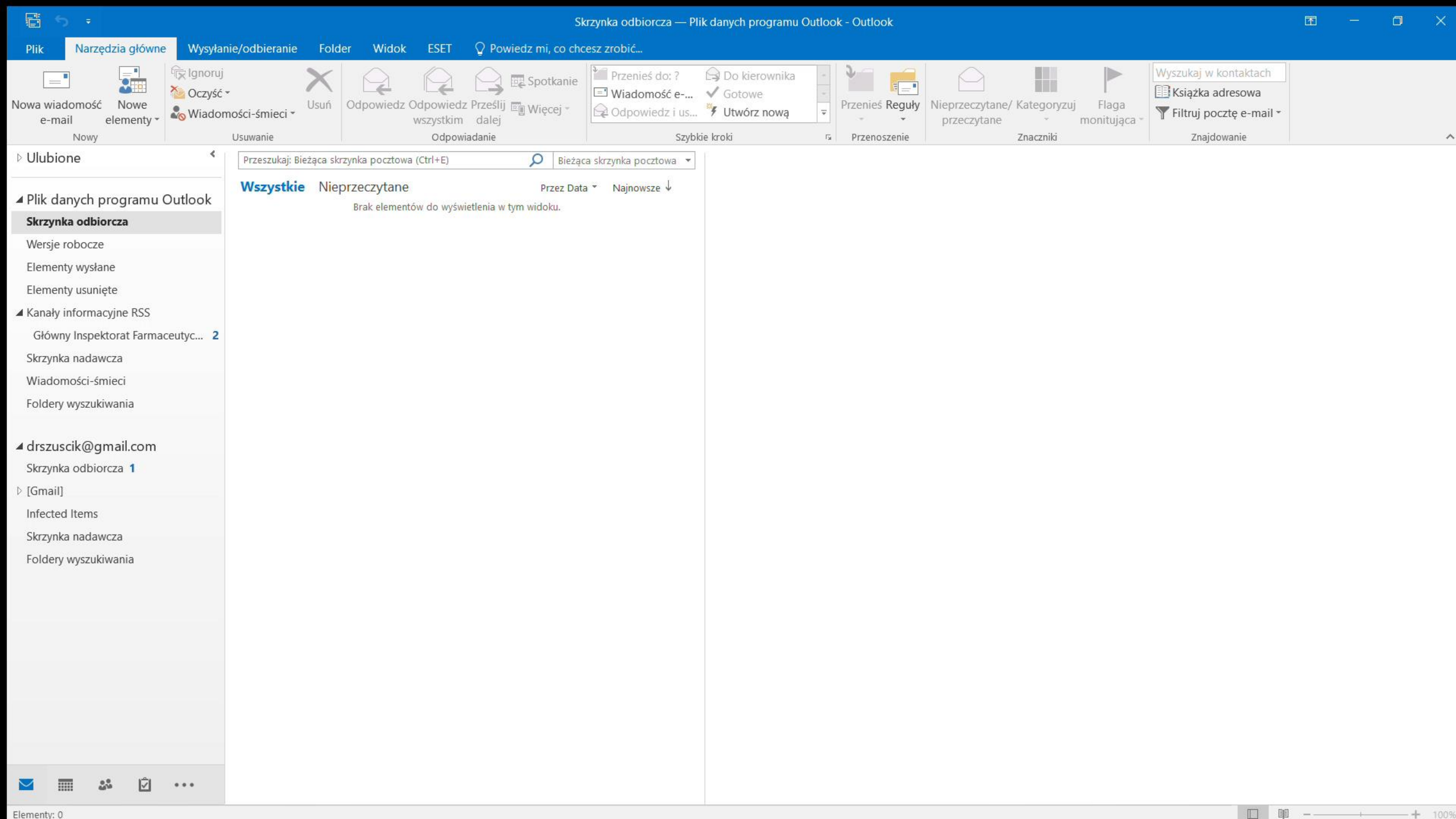
Prelegent: Karolina Szuścik; Kamsoft S.A.

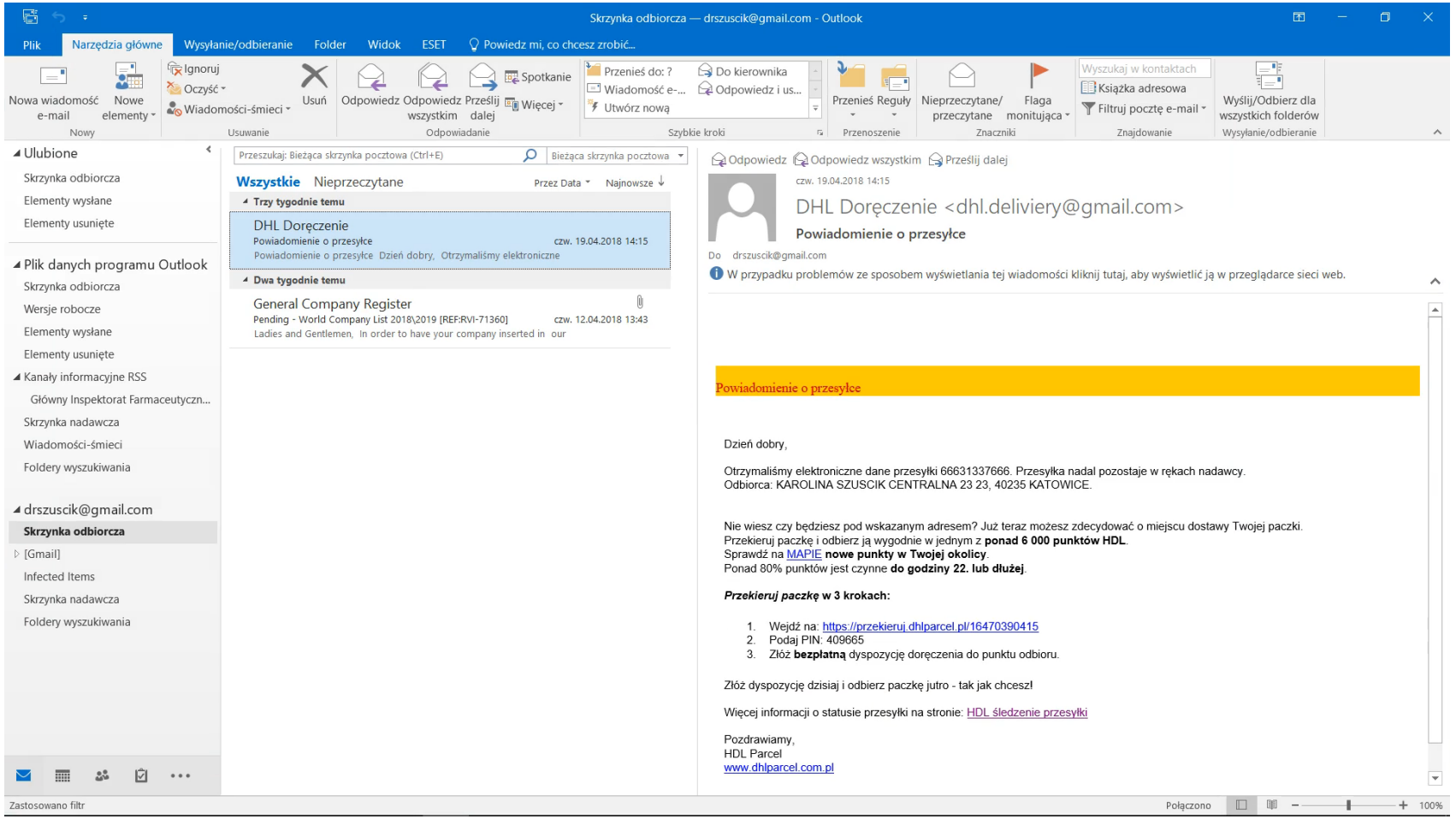
Prelegent: Łukasz Markowski; Kamsoft S.A.

Prelegent: Bartłomiej Syryjczyk; Kamsoft S.A.

OSOZ - OTWARTY SYSTEM OCHRONY ZDROWIA


Gabinet Lekarski 2018
Funkcje podstawowe
Elementy wizyty
Kasa
Bazy
eZLA
Wizyta
Badania okresowe
Wizyta stara wersja
Zawieszone wizyty
Wizyta
Dokument z pliku/Skanuj
HZiCh
Podpisana
Dokumentacja medyczna
Zgony
Kalendarz szczepień
Zlecenie na leki
Inne
Wyd.pustych recept
Wydruk wizyt
Wydruki
SA
2018-03-26 18:01
Gabinet Lekarski 2018
2017.03.0.07
Op.: KS
Lek.: KS
Gab.: GLEK
Por.: PO
Podm.: KS


Skrzynka odbiorcza — Plik danych programu Outlook - Outlook
Plik
Narzędzia główne
Wysyłanie/odbieranie
Folder
Widok
ESET
Powiedz mi, co chcesz zrobić...
Nowa wiadomość e-mail
Nowe elementy
Nowy
Ignoruj
Oczyść
Wiadomości-śmieci
Usuń
Usuwanie
Odpowiedz
Odpowiedz wszystkim
Prześlij dalej
Spotkanie
Więcej
Odpowiadanie
Przenieś do: ?
Wiadomość e-...
Odpowiedz i us...
Do kierownika
Gotowe
Utwórz nową
Szybkie kroki
Przenieś
Reguły
Przenoszenie
Nieprzeczytane/ przeczytane
Kategoryzuj
Flaga monitująca
Znaczniki
Wyszukaj w kontaktach
Książka adresowa
Filtruj pocztę e-mail
Znajdowanie
Ulubione
Plik danych programu Outlook
Skrzynka odbiorcza
Wersje robocze
Elementy wysłane
Elementy usunięte
Kanały informacyjne RSS
Główny Inspektorat Farmaceutyc... 2
Skrzynka nadawcza
Wiadomości-śmieci
Foldery wyszukiwania
drszuscik@gmail.com
Skrzynka odbiorcza 1
[Gmail]
Infected Items
Skrzynka nadawcza
Foldery wyszukiwania
Przeszukaj: Bieżąca skrzynka pocztowa (Ctrl+E)
Bieżąca skrzynka pocztowa
Wszystkie
Nieprzeczytane
Przez Data
Najnowsze
Brak elementów do wyświetlenia w tym widoku.
Elementy: 0
100%


Skrzynka odbiorcza — drszuscik@gmail.com - Outlook
Plik
Narzędzia główne
Wysyłanie/odbieranie
Folder
Widok
ESET
Powiedz mi, co chcesz zrobić...
Nowa wiadomość e-mail
Nowe elementy
Ignoruj
Oczyść
Wiadomości-śmieci
Usuń
Odpowiedz
Odpowiedz wszystkim
Prześlij dalej
Spotkanie
Więcej
Przenieś do: ?
Wiadomość e-...
Utwórz nową
Do kierownika
Odpowiedz i us...
Przenieś
Reguły
Nieprzeczytane/ przeczytane
Flaga monitująca
Wyszukaj w kontaktach
Książka adresowa
Filtruj pocztę e-mail
Wyślij/Odbierz dla wszystkich folderów
Nowy
Usuwanie
Odpowiadanie
Szybkie kroki
Przenoszenie
Znaczniki
Znajdowanie
Wysyłanie/odbieranie
Ulubione
Skrzynka odbiorcza
Elementy wysłane
Elementy usunięte
Plik danych programu Outlook
Skrzynka odbiorcza
Wersje robocze
Elementy wysłane
Elementy usunięte
Kanały informacyjne RSS
Główny Inspektorat Farmaceutyczn...
Skrzynka nadawcza
Wiadomości-śmieci
Foldery wyszukiwania
drszuscik@gmail.com
Skrzynka odbiorcza
[Gmail]
Infected Items
Skrzynka nadawcza
Foldery wyszukiwania
Przeszukaj: Bieżąca skrzynka pocztowa (Ctrl+E)
Bieżąca skrzynka pocztowa
Wszystkie
Nieprzeczytane
Przez Data
Najnowsze
Trzy tygodnie temu
DHL Doręczenie
Powiadomienie o przesyłce
czw. 19.04.2018 14:15
Powiadomienie o przesyłce Dzień dobry, Otrzymaliśmy elektroniczne
Dwa tygodnie temu
General Company Register
Pending - World Company List 2018\2019 [REF:RVI-71360]
czw. 12.04.2018 13:43
Ladies and Gentlemen, In order to have your company inserted in our
Odpowiedz
Odpowiedz wszystkim
Prześlij dalej
czw. 19.04.2018 14:15
DHL Doręczenie <dhl.deliviery@gmail.com>
Powiadomienie o przesyłce
Do drszuscik@gmail.com
W przypadku problemów ze sposobem wyświetlania tej wiadomości kliknij tutaj, aby wyświetlić ją w przeglądarce sieci web.
Powiadomienie o przesyłce
Dzień dobry,
Otrzymaliśmy elektroniczne dane przesyłki 66631337666. Przesyłka nadal pozostaje w rękach nadawcy.
Odbiorca: KAROLINA SZUSCIK CENTRALNA 23 23, 40235 KATOWICE.
Nie wiesz czy będziesz pod wskazanym adresem? Już teraz możesz zdecydować o miejscu dostawy Twojej paczki.
Przekieruj paczkę i odbierz ją wygodnie w jednym z ponad 6 000 punktów HDL.
Sprawdź na MAPIE nowe punkty w Twojej okolicy.
Ponad 80% punktów jest czynne do godziny 22. lub dłużej.
Przekieruj paczkę w 3 krokach:
1. Wejdź na: https://przekieruj.dhlparcel.pl/16470390415
2. Podaj PIN: 409665
3. Złóż bezpłatną dyspozycję doręczenia do punktu odbioru.
Złóż dyspozycję dzisiaj i odbierz paczkę jutro - tak jak chcesz!
Więcej informacji o statusie przesyłki na stronie: HDL śledzenie przesyłki
Pozdrawiamy,
HDL Parcel
www.dhlparcel.com.pl
Zastosowano filtr
Połączono
100%

Wszystkie pliki na tym komputerze zostały zaszyfrowane przy użyciu algorytmu RSA-2048

Aby odzyskać swoje dane proszę działać zgodnie z poniższą instrukcją:

1. Zapłać 0.15 BTC na adres: 13QtzNuN8T7n3BykszFoGBDgDwerDwyHmi1z*

2. Wyślij ID swojego portfela Bitcoin na poniższy adres mail: 12345@posteo.net

Pamiętaj ! Na zapłacenie masz tylko 96 h !

*Jeżeli nie wiesz w jaki sposób dokonać opłaty pod tym adresem znajdziesz krótką instrukcję
https://blockchain.info/howtocreatewallet

Definicja ransomware

Źródło: PixaBay

Ransomware (ang. ransomware - zbitka słów **ransom** "okup" i soft**ware** "oprogramowanie") – typ szkodliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

ATTACK ORIGINS

#	COUNTRY
43	United States
17	Czech Republic
15	China
12	Ukraine
4	India
3	Vietnam
2	Romania
2	Netherlands
2	Japan

ATTACK TYPES

#	PORT	SERVICE TYPE
38	25	unknown
29	23	unknown
17	5900	unknown
9	8080	unknown
3	445	unknown
2	137	unknown
2	80	unknown
1	9794	unknown
1	50864	unknown

ATTACK TARGETS

#	COUNTRY
74	United States
31	United Arab Emirates
2	Thailand
2	Hong Kong
2	Spain
1	Saudi Arabia
1	Mexico
1	France

LIVE ATTACKS

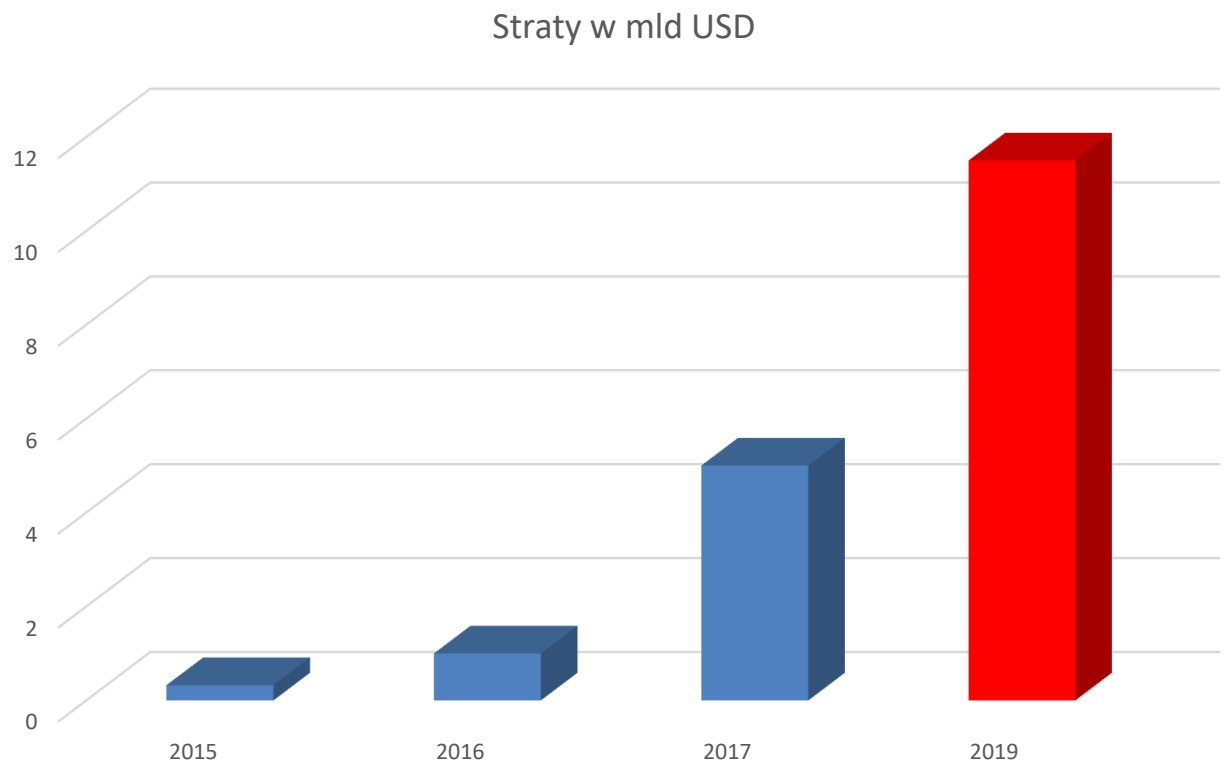
TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
13:28:46.250	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	unknown	8080
13:28:46.248	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	unknown	8080
13:28:45.974	Microsoft Corporation	65.55.169.245	Washington, US	De Kalb Junctio...	unknown	25
13:28:45.772	Microsoft Corporation	157.56.111.249	Redmond, US	De Kalb Junctio...	unknown	25
13:28:45.508	Microsoft Corporation	207.46.100.251	Redmond, US	De Kalb Junctio...	unknown	25
13:28:45.284	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	unknown	8080
13:28:44.772	Microsoft Corporation	207.46.100.247	Redmond, US	De Kalb Junctio...	unknown	25
13:28:44.624	Berca Global Access	223.164.2.22	Jakarta, ID	Lynnwood, US	unknown	49638
13:28:44.076	Microsoft Corporation	65.55.169.249	Washington, US	De Kalb Junctio...	unknown	25

HOME

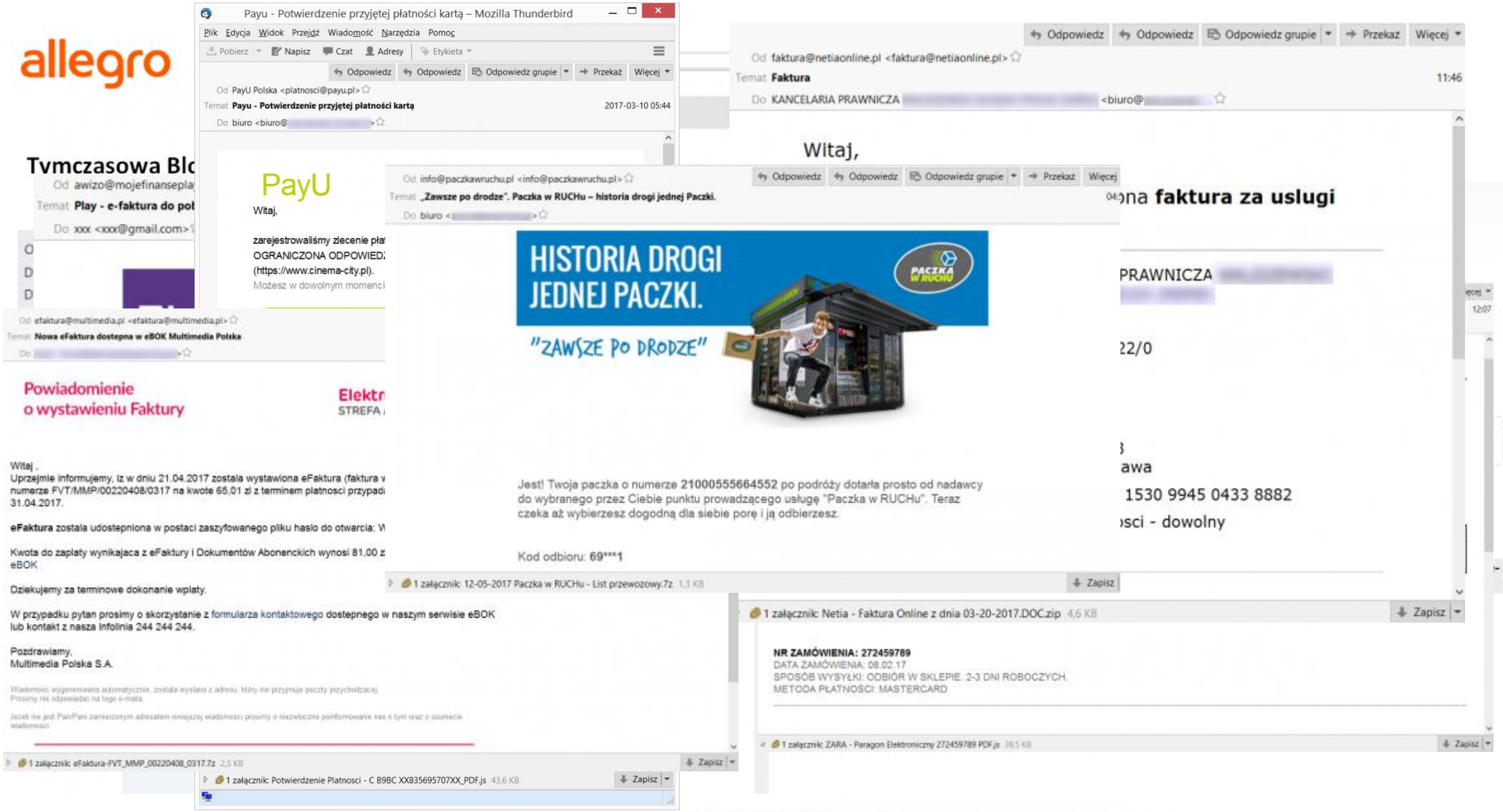
EXPLORE

WHY NORSE?

Statystyki



Analiza przypadku



Analiza wiadomości

wt. 01.03.2016 03:02

mBank <cenker@chipshare.com> 1

Nowa wiadomosc mBank

Do [redacted]

Data: 29.02.2016 r.

Dostęp do serwisu transakcyjnego mBank został tymczasowo zablokowany!

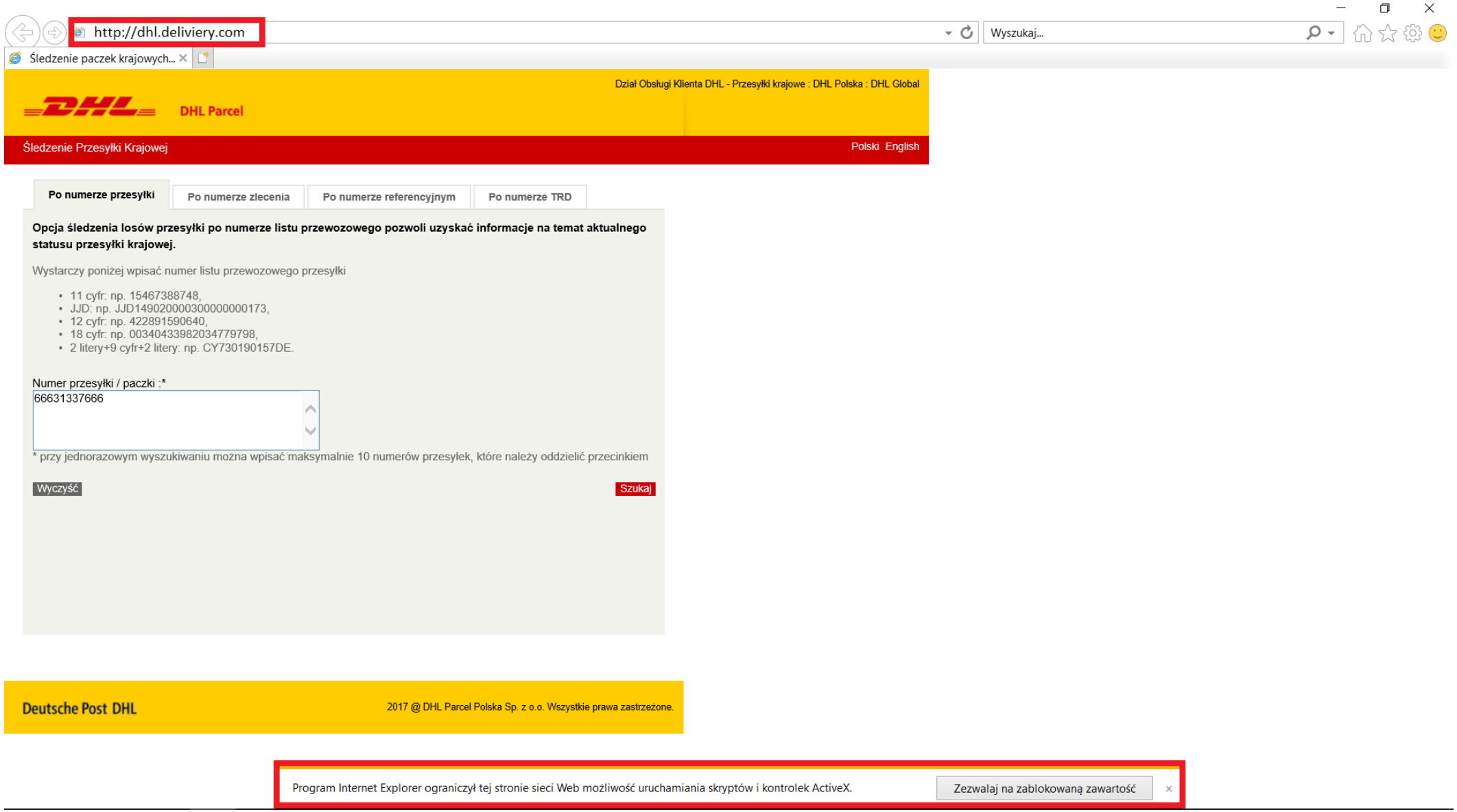
W trosce o bezpieczeństwo naszych klientów zablokowaliśmy konto w systemie mBank, powodem jest nieautoryzowany dostęp do konta.
W celu uzyskania informacji oraz odblokowania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

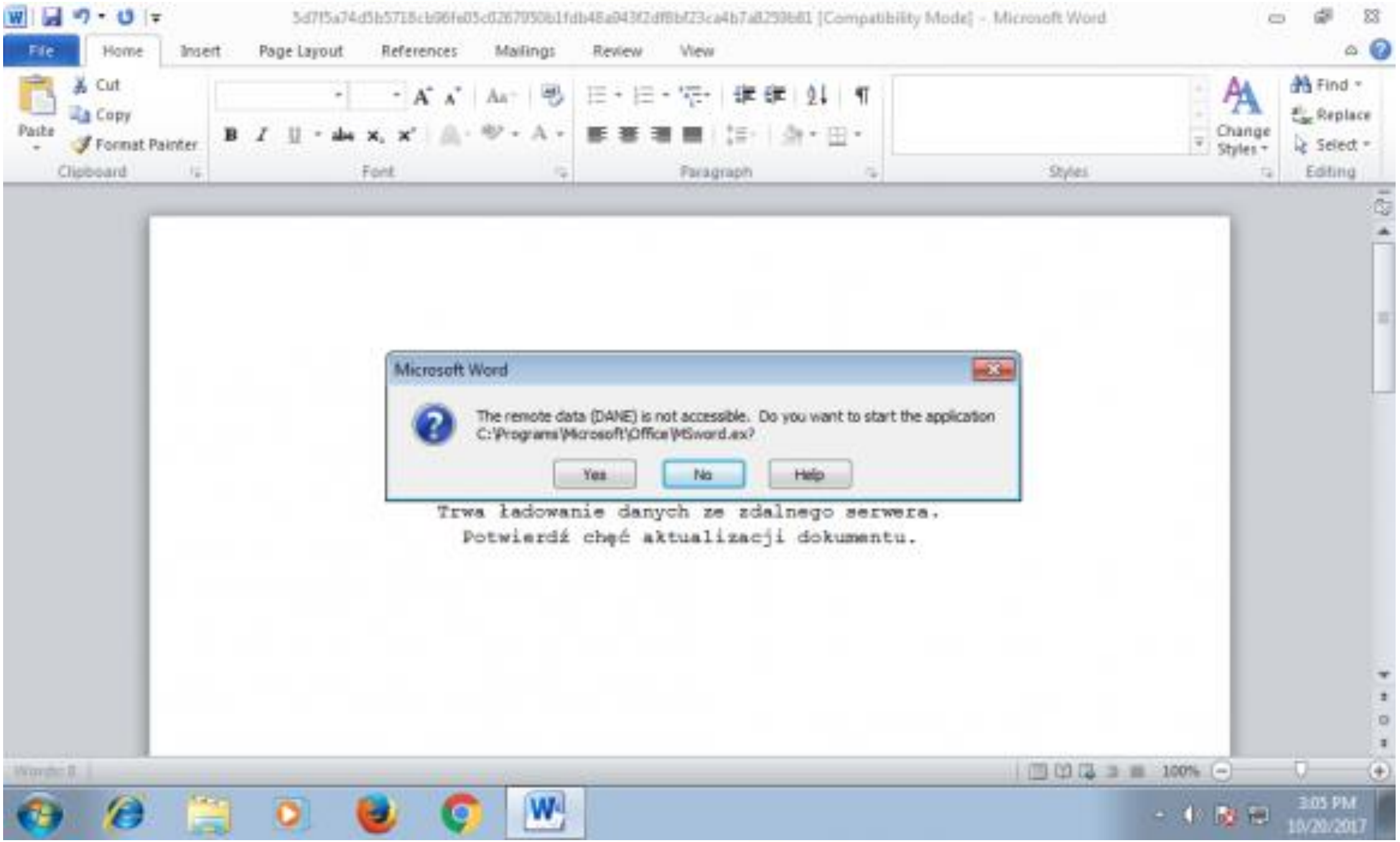
2 **www.online.mbank.pl** → 3 http://mbank-autoryzacja.pw/?email=[redacted]

Serdecznie pozdrawiamy,
Zespół mBank

W przypadku jakichkolwiek pytań prosimy o kontakt z mLinia 801 300 300

Ten e-mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać. mBank S.A. z siedzibą w Warszawie, ul. Senatorska 18, 00-950 Warszawa, Oddział Bankowości Mobilnej w Łodzi, zarejestrowany przez Sąd Rejonowy dla m. st. Warszawy XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000025237, posiadający numer identyfikacji podatkowej NIP: 526-021-50-88, o wpłaconym w całości kapitale zakładowym, którego wysokość według stanu na dzień 01.01.2016 r. wynosi 168.955.696 zł (w całości wpłacony).


http://dhl.deliviery.com
Wyszukaj...
Śledzenie paczek krajowych...
Dział Obsługi Klienta DHL - Przesyłki krajowe : DHL Polska : DHL Global
DHL Parcel
Śledzenie Przesyłki Krajowej
Polski English
Po numerze przesyłki
Po numerze zlecenia
Po numerze referencyjnym
Po numerze TRD
Opcja śledzenia losów przesyłki po numerze listu przewozowego pozwoli uzyskać informacje na temat aktualnego statusu przesyłki krajowej.
Wystarczy poniżej wpisać numer listu przewozowego przesyłki
11 cyfr: np. 15467388748,
JJD: np. JJD14902000030000000173,
12 cyfr: np. 422891590640,
18 cyfr: np. 00340433982034779798,
2 litery+9 cyfr+2 litery: np. CY730190157DE.
Numer przesyłki / paczki :*
66631337666
* przy jednorazowym wyszukiwaniu można wpisać maksymalnie 10 numerów przesyłek, które należy oddzielić przecinkiem
Wyczyść
Szukaj
Deutsche Post DHL
2017 @ DHL Parcel Polska Sp. z o.o. Wszystkie prawa zastrzeżone.
Program Internet Explorer ograniczył tej stronie sieci Web możliwość uruchamiania skryptów i kontrolek ActiveX.
Zezwalaj na zablokowaną zawartość


Microsoft Word
The remote data (DANE) is not accessible. Do you want to start the application C:\Programs\Microsoft\Office\MSword.ex?
Yes
No
Help
Trwa ładowanie danych ze zdalnego serwera.
Potwierdź chęć aktualizacji dokumentu.


Wana Decrypt0r 2.0
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
Check Payment
Decrypt

Środki zaradcze

- „Cyber higiena”
- Kopie bezpieczeństwa offline
- Aktualizacje i poprawki oprogramowania i systemu operacyjnego
- Zaufane oprogramowanie antywirusowe – niekoniecznie musi ochronić przed nowymi zagrożeniami

Jeśli już doszło do infekcji…

- Szyfrowanie trwa, więc jest szansa je przerwać i ocalić część plików
- Nie płacić!
- Czas leczy rany…

Kilka przykładów

Hollywoodzkie centrum medyczne (Hollywood Presbyterian Medical Center) sparaliżowane przez komputerowych przestępców. Zapłacili okup 17’000 USD (40 XBT).

W niemieckim Neuss w Lukas Hospital udało się odzyskać dane z kopii bezpieczeństwa bez płacenia okupu, ale prace pochłonęły kilka tygodni

Locky zaatakował Whanganui District Health Board (Nowa Zelandia). Nie zapłacono okupu. Wzmocniono procedury i zainwestowano w dodatkowe zabezpieczenia.

Wśród ofiar ataku WannaCry w 2017 r. był m. in. brytyjski system służby zdrowia (National Health Service), gdzie zainfekowanych zostało nawet do 70’000 urządzeń.

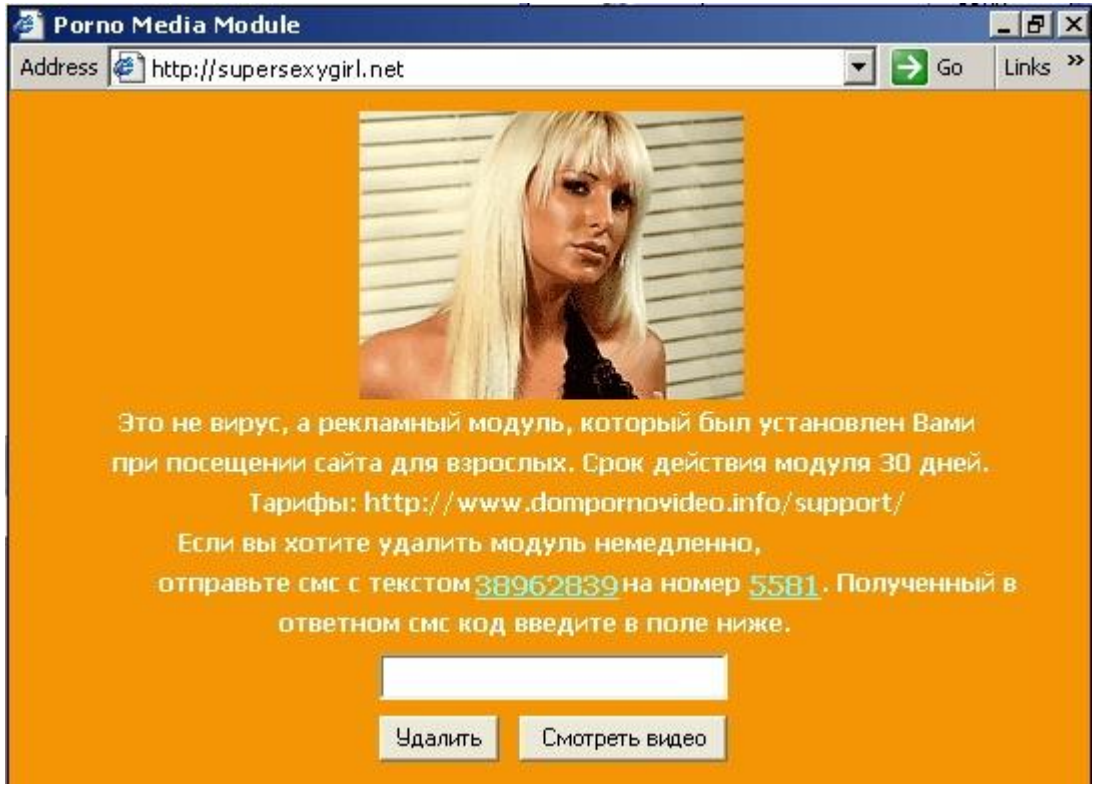
Historia

Pierwszym znanym oprogramowaniem szantażującym był „AIDS”, napisany w 1989. Jego kod był odpowiedzialny za ukrywanie plików na dysku i szyfrowanie ich nazw, a także za wyświetlanie informacji, że licencja użytkownika na korzystanie z konkretnych plików wygasła. Ofiara była proszona o dokonanie wpłaty w wysokości 189$ na konto bankowe w celu uzyskania programu do usunięcia infekcji.

Źródło: PixaBay

WinLock

- 2010 r.
- Nie używał szyfrowania, blokada komputera
- Rodzaj płatności: SMS premium
- Cel: Rosja i okolice
- 16 milionów USD zarobku

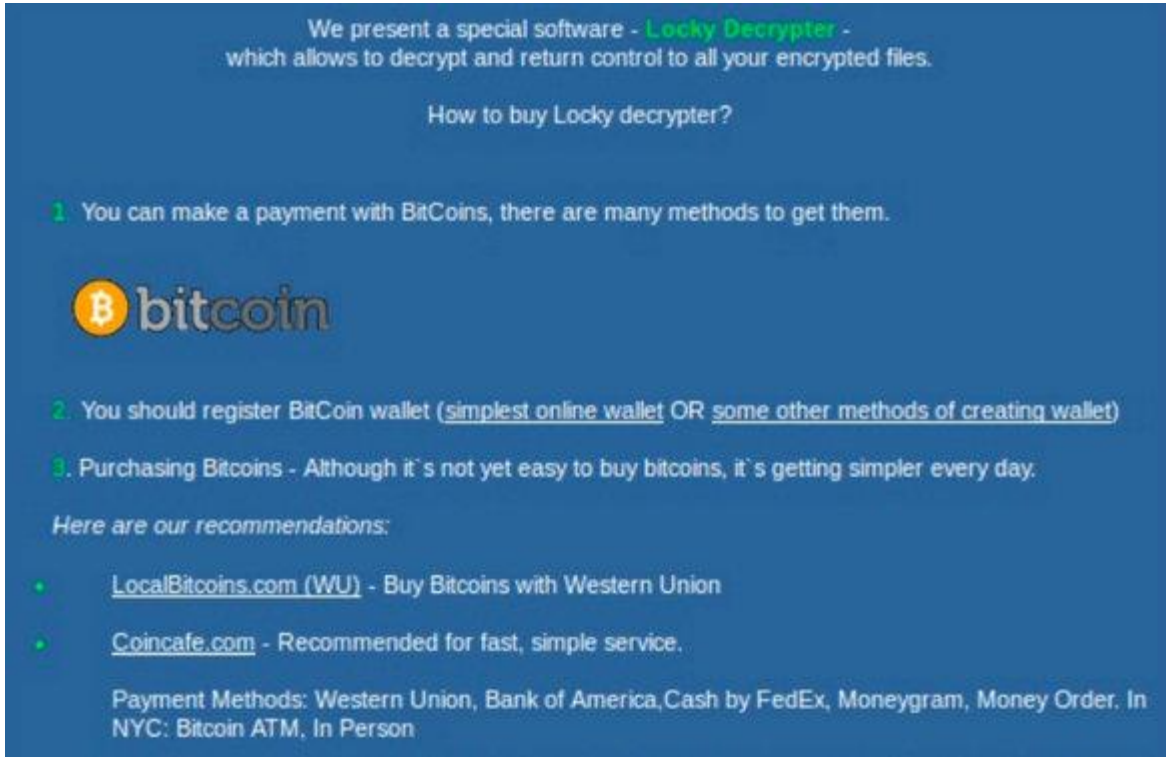


CryptoLocker

- 2013 – 2014 r.
- wykorzystywał platformę waluty cyfrowej Bitcoin do pozyskiwania okupu
- twórcy CryptoLockera otrzymali ok. 42’000 XBT od zainfekowanych użytkowników (1% ofiar zapłaciło)
- generował 2048-bitową parę kluczy RSA
- badacze opublikowali szczepionkę

Locky

- Luty 2016 r.
- 90’000 komputerów w ciągu dnia
- Ukryty w dokumencie Word

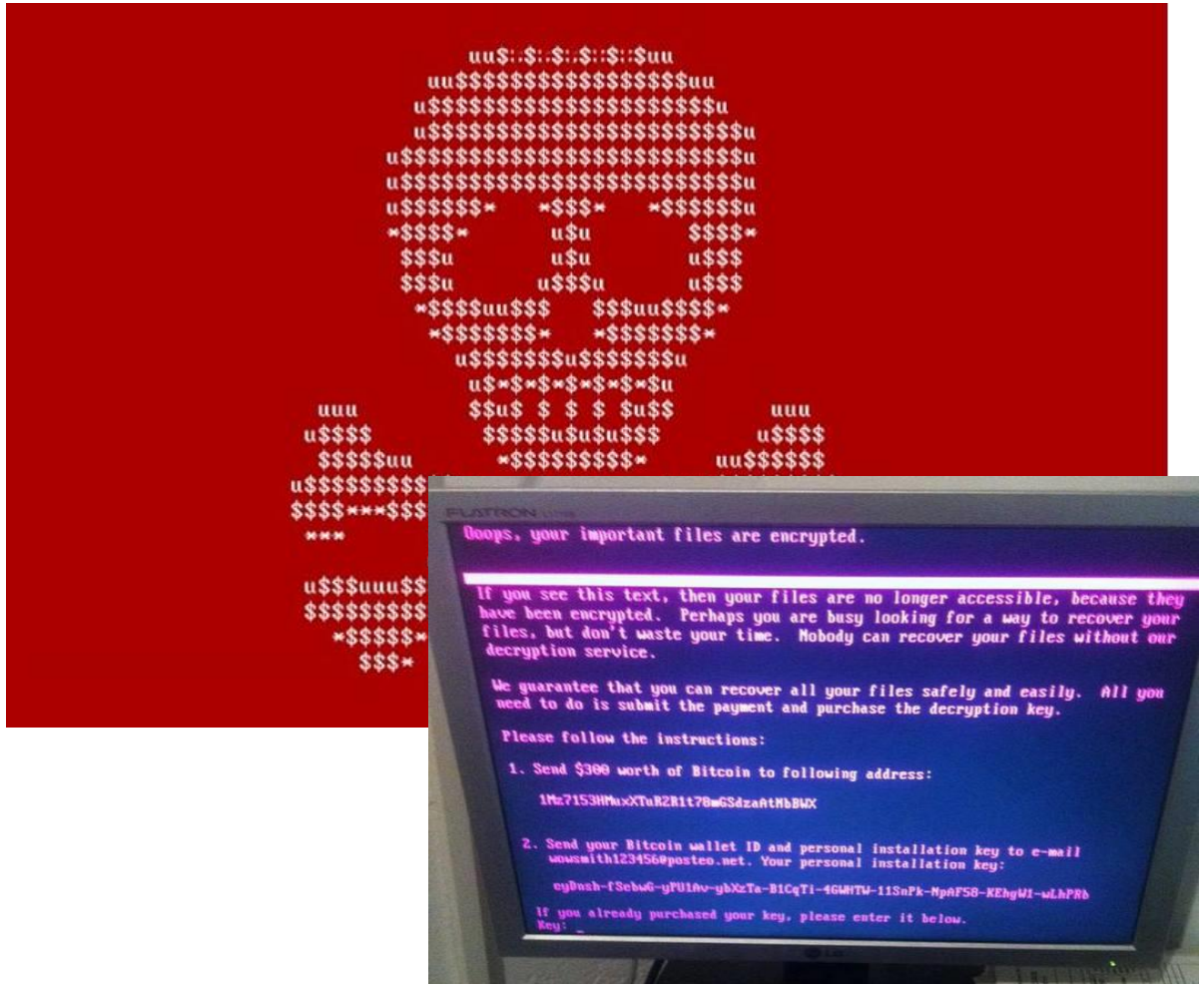


WannaCry

- Maj 2017 r.
- 230’000 komputerów w 150 krajach
- Bazował na lukach, które wyciekły z NSA (afera Snowden’a)
- Żądał 300 USD od komputera
- Wśród ofiar ataku m. in. brytyjski system służby zdrowia (National Health Service), gdzie zainfekowanych zostało nawet do 70’000 urządzeń
- Szpitale w Indonezji, na Słowacji

Petya

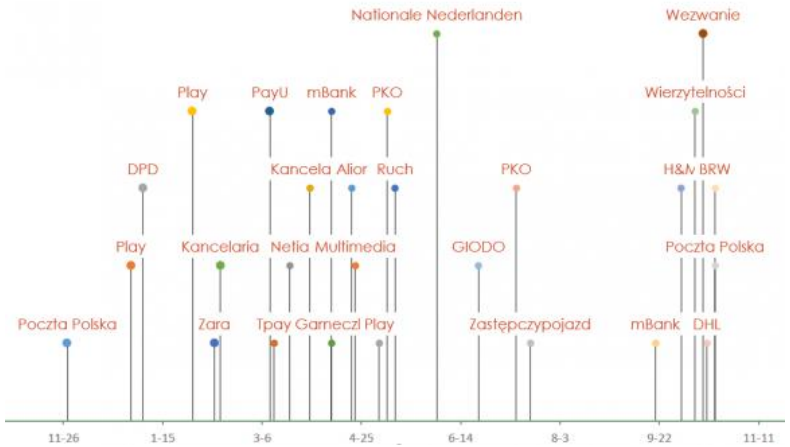
- Podobne rozprzestrzenianie jak WannaCry
- Ślady już w marcu 2016 r.; globalny atak w czerwcu 2017 r.
- Główny obszar ataku to Ukraina i Rosja, ale także Francja, Niemcy, Włochy, Polska i USA
- Nazwany najbardziej destrukcyjnym cyberatakiem
- Ofiarą m. in. system monitorowania promieniowania w elektrowni w Czarnobylu, a także firma farmaceutyczna Merck & Company i amerykański operator szpitali Heritage Valley Health System
- Princeton Community Hospital zezłomował i wymienił całą infrastrukturę w działaniu naprawczym
- Twórca (?) udostępnił po czasie narzędzie odszyfrowujące dyski/pliki



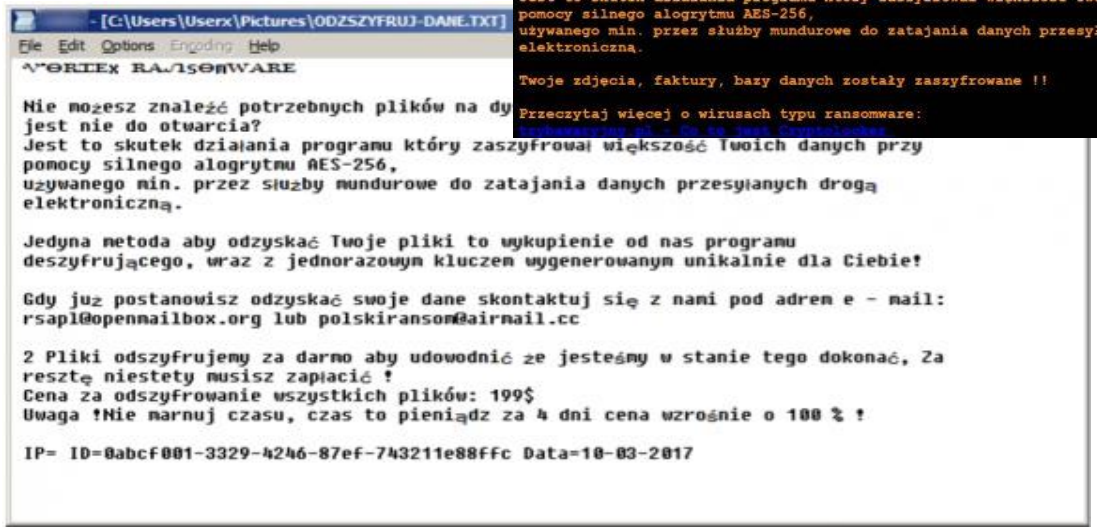
Źródło: Z3S

Tomasz T. aka Thomas

- Sześć lat działalności
- Miliony wysłanych wiadomości
- Tysiące zainfekowanych komputerów
- Setki ofiar ransomware (Polski Ransomware / Vortex / Flotera)
- Zatrzymany 14 marca 2018 r. przez policję



Źródło: Z3S



DZIĘKUJĘ ZA UWAGĘ

THANK YOU FOR YOUR ATTENTION