



KOMENDA GŁÓWNA POLICJI

Biuro Spraw Wewnętrznych
Krajowe Centrum Informacji Kryminalnych



Wspierane i Chronione przez 

IP: 


Kraj: PL Poland

Region: Mazowieckie

Miasto: Warsaw

ISP: 

System Operacyjny: Windows XP (32-bit)

Nazwa Użytkownika: 



UWAGA! Pański komputer jest zablokowany ze co najmniej jednego z powodów podanych poniżej.

Pan/Pani naruszył/a «Ustawę o prawach autorskich i prawach pokrewnych» (video, muzyka, oprogramowanie) oraz nielegalnie używał/a lub rozpowszechniał/a treści chronionych prawem autorskim, tym samym naruszając artykuł 128 Kodeksu Karnego Rzeczypospolitej Polskiej.

Artykuł 128 Kodeksu Karnego przewiduje karę grzywny od 200 do 500 minimalnych wynagrodzeń lub pozbawienia wolności od 2 do 8 lat.

Pan/Pani oglądał/a lub rozpowszechniał zakazane treści pornograficzne (pornografia dziecięca/zoofilia itp.), w taki sposób naruszając artykuł 202 Kodeksu Karnego Rzeczypospolitej Polskiej.

Kod PIN

Wartość

500

1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---

[Opłacić Ukash](#)

[Opłacić PaySafe](#)

Gdzie mogę nabyć kupon Ukash?

Możesz nabyć Ukash w jednym z tysięcy punktów na świecie, przez Internet, przez portfel, w bankomacie.



www.dotPay.pl - Zakup kuponu w serwisie www.dotPay.pl



ePay - Ukash możesz kupić w wybranych sklepach z logo ePay.



Apollo - Sprawdź Warunki Ukash uzyskasz kod Ukash lub użyjesz go

Antimalware Webapp Solution - Agenda

- Co to jest ten malware?
- Przykłady ataków
- Jak z nim walczyć
- Dlaczego to już nie działa
- No i co z tym zrobić

Malware czyli złośliwe oprogramowanie

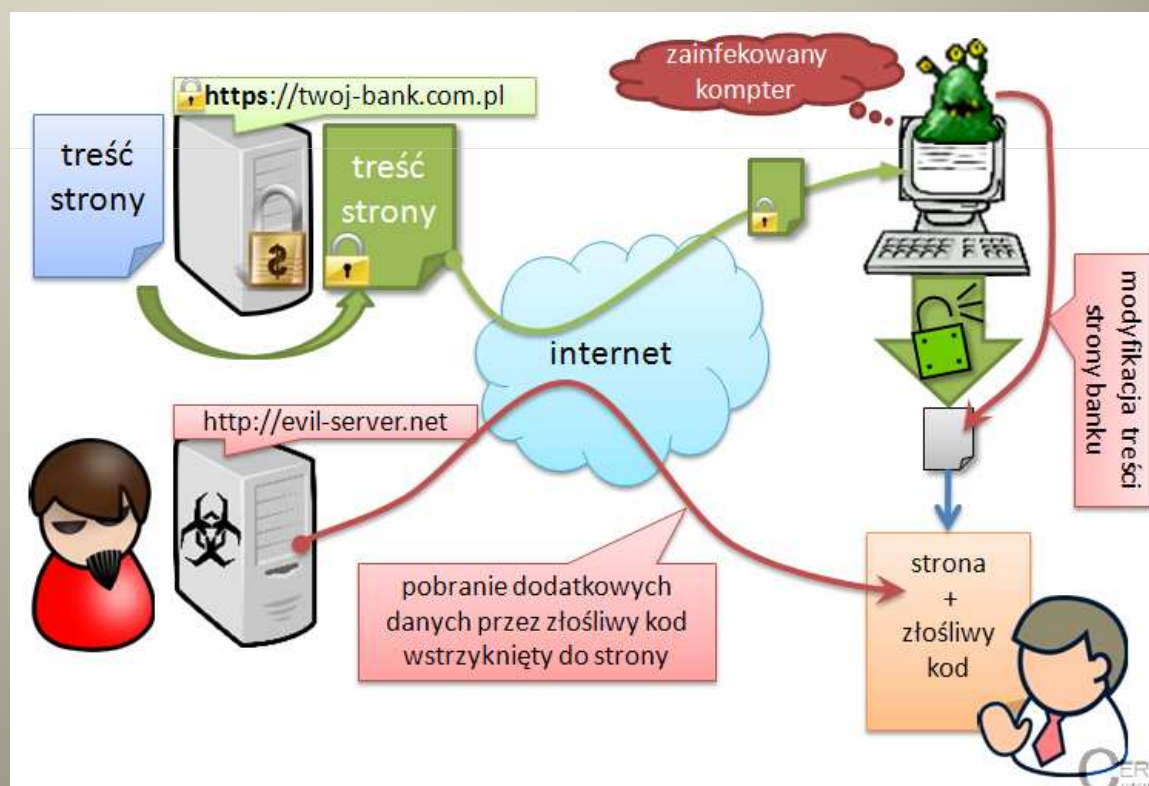


Malware – na przykładzie bankowości

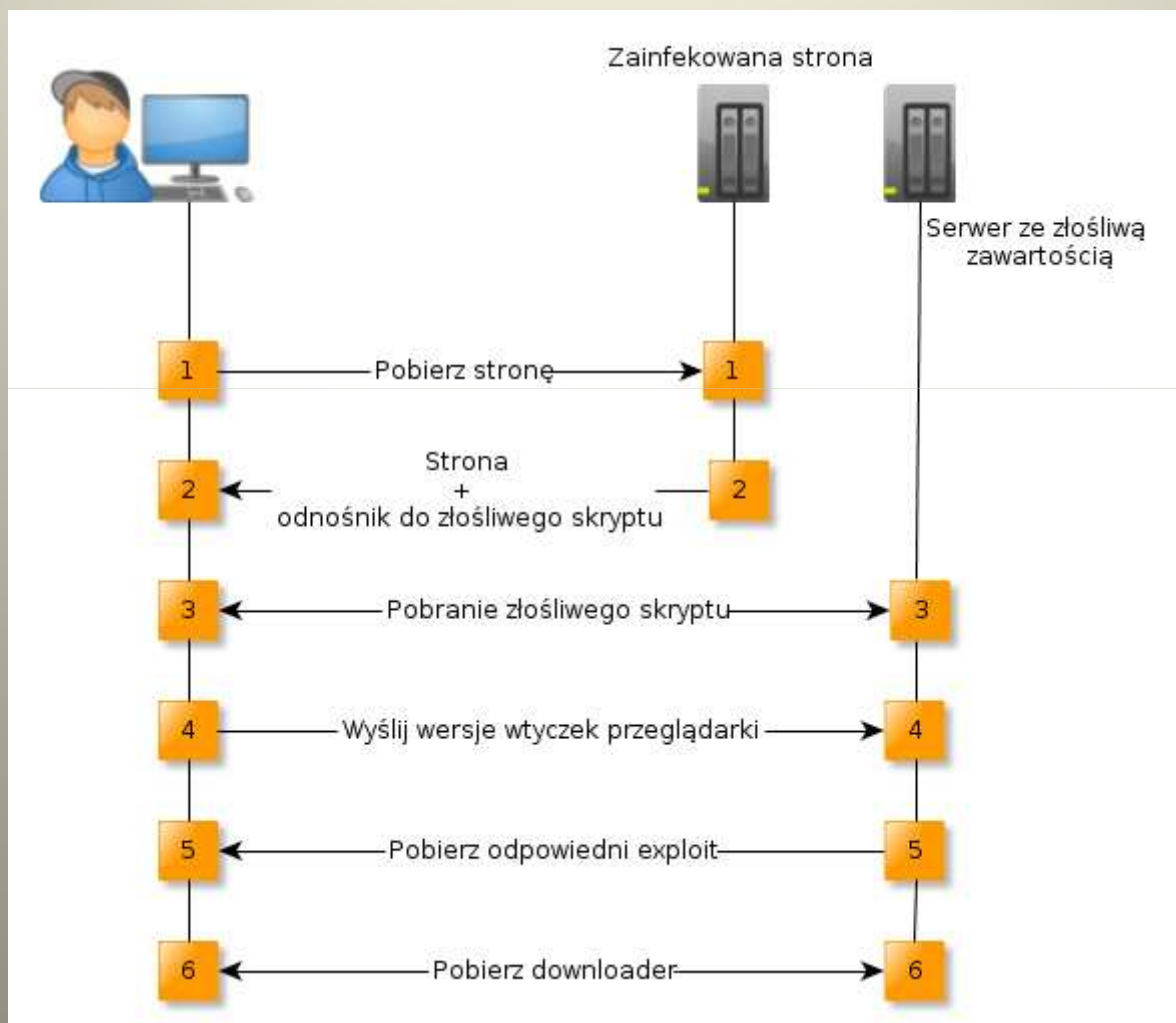
- 2007 pierwsze sygnały o nowym trojanie atakującym bankowość elektroniczną (keylogger), w Polsce 2011
- 2011 wiosna, upublicznienie kodu źródłowego
- 2011 atak na bankowość mobilną (SpyEye)
- 2012 ZEUS P2P/Citadel
- 2013 ZitMo

Atak z wykorzystaniem Malware

- Infekcja stacji klienta
- Zebranie NIK/PIN danych o koncie (Webinject)
- Socjotechnika

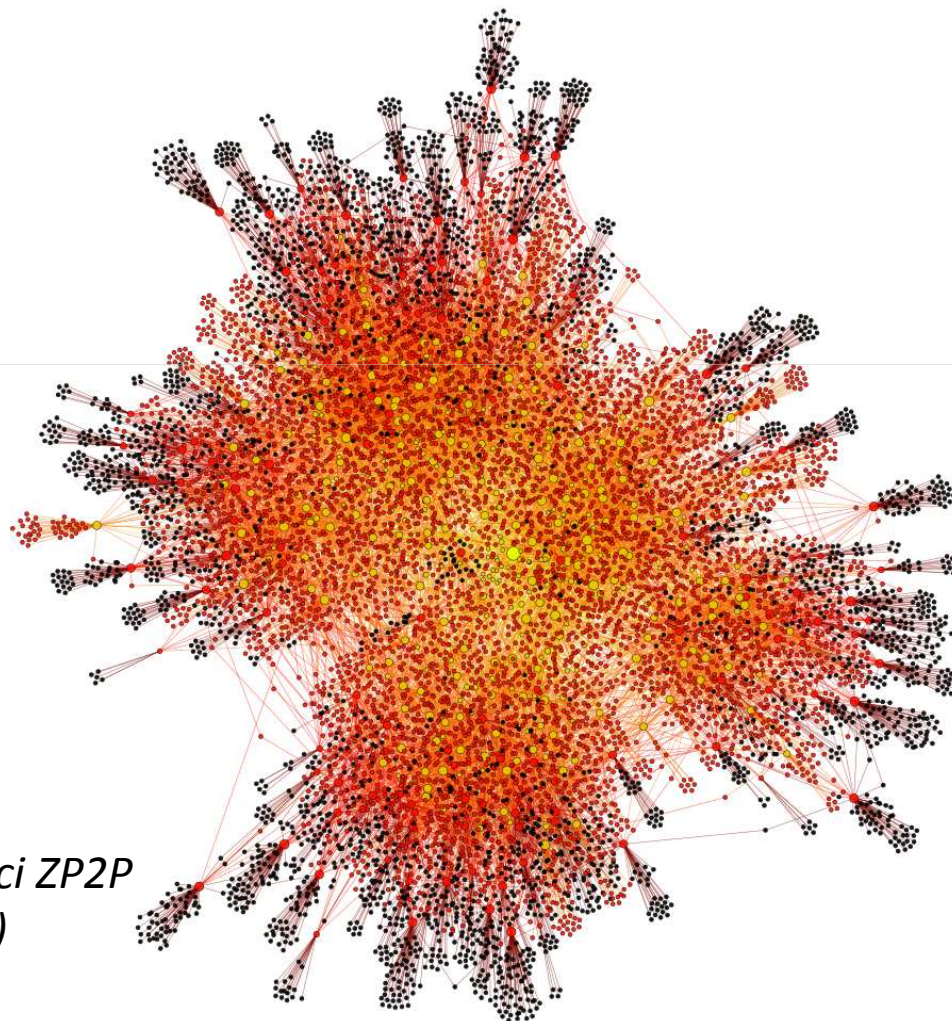


Ataki typu ransomware



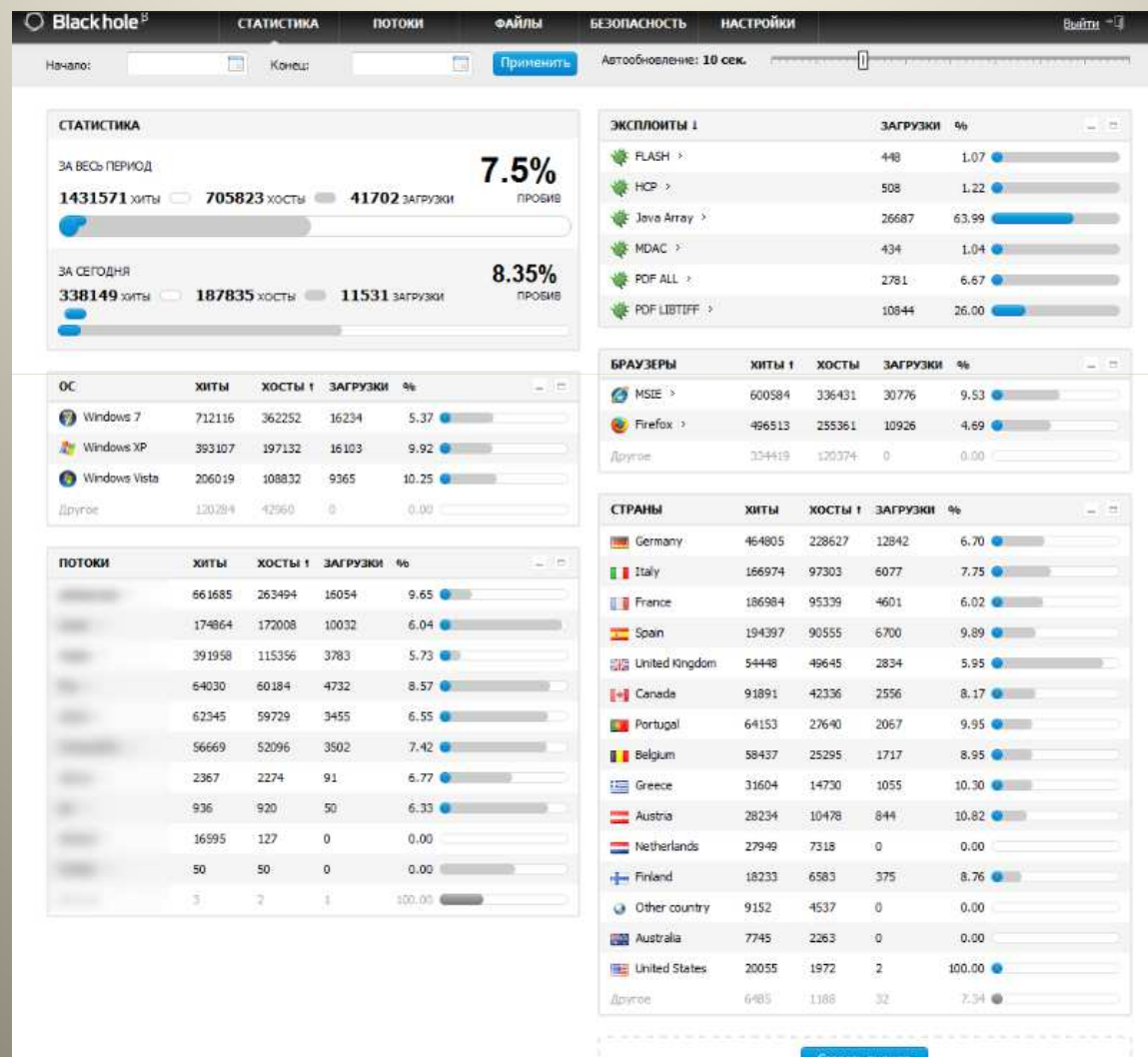
źródło: cert.pl

ZEUS – P2P

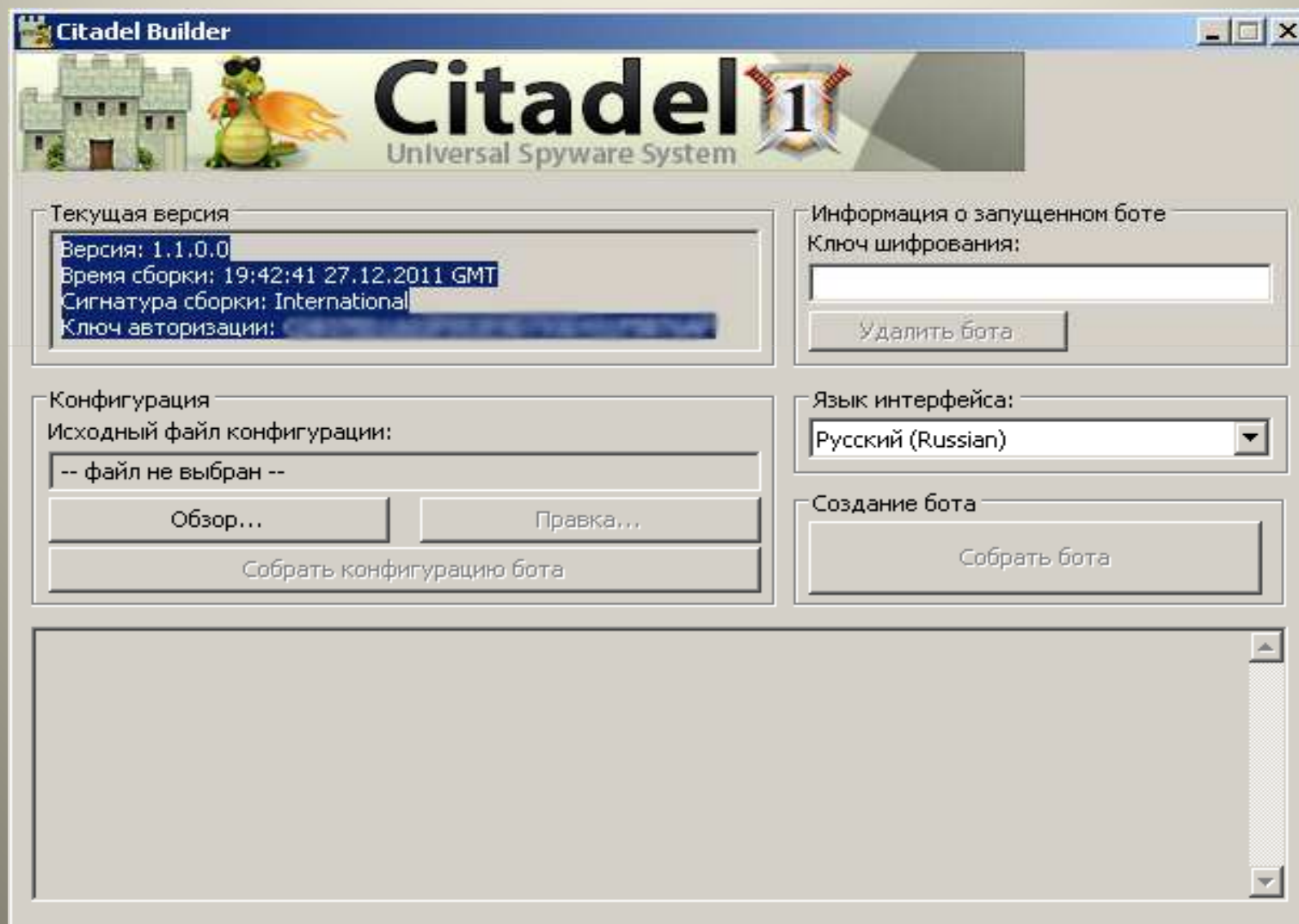


Wizualizacja sieci ZP2P
(10 000 węzłów)

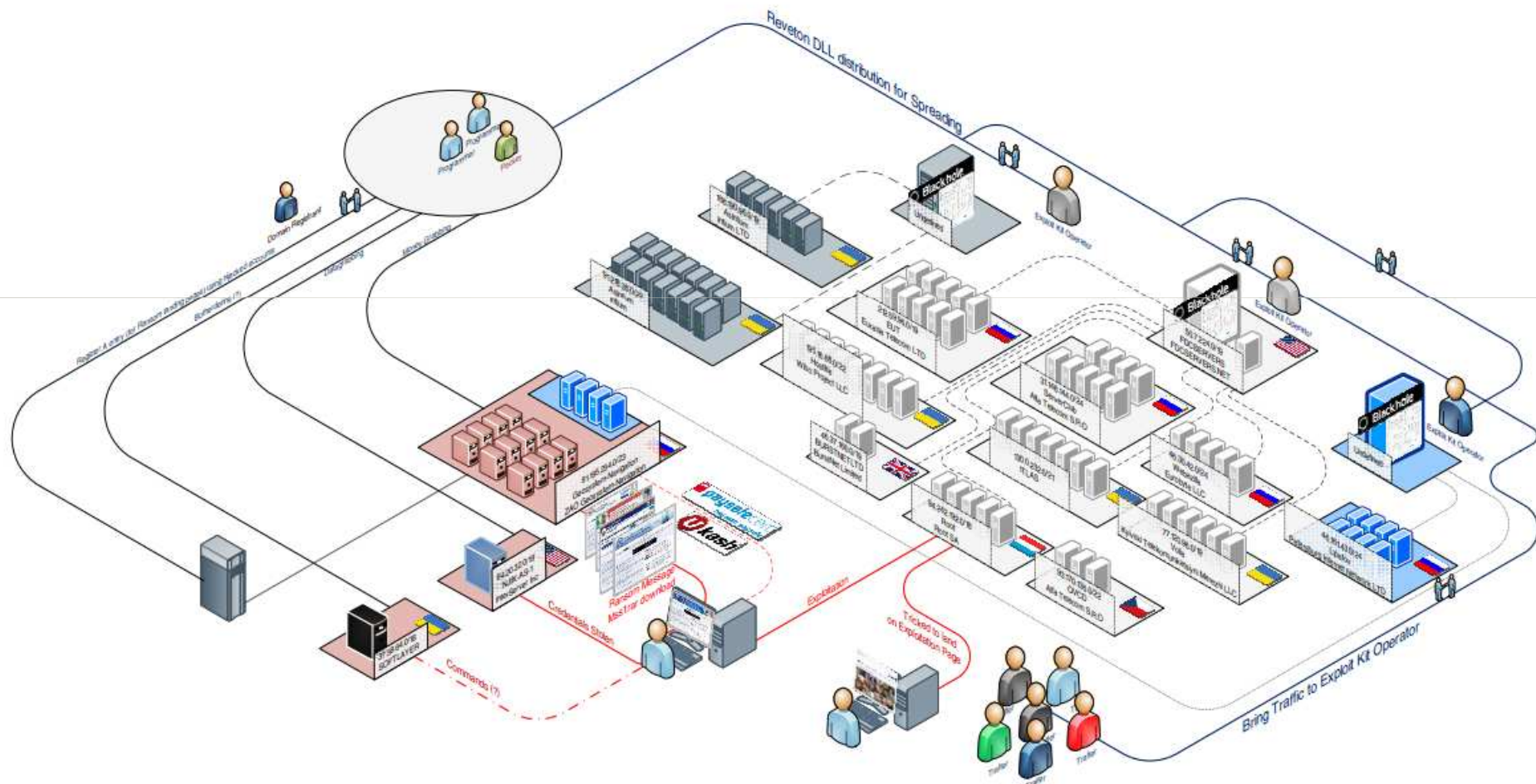
ZEUS - blackhole



ZEUS - Citadel



Ransomware ala Reveton (Citadel inside)



Webinject

```
<rule id=457>
  <condition type=AND>(^http.*?://.*?facebook\..*?/.*) </condition>
  <condition type=NOT> (\.(gif|png|jpg|css|swf)($|\?)) </condition>
  <injects>
    [[[ DATA-MATCH ]]]
    (<html(<inject>))
    [[[ DATA-END ]]]
    [[[ DATA-INJECT ]]]
    style="display:none;"
    [[[ DATA-END ]]]

    [[[ DATA-MATCH ]]]
    (<head.*?>(<inject>))
    [[[ DATA-END ]]]
    [[[ DATA-INJECT ]]]
    <script>window.onerror = function (msg){return true};var attr = true;</script>
    [[[ DATA-END ]]]
  </injects>
</rule>
```

Socjotechnika

Ważny Klient!

Dzisiaj na Wasze konto został dokonany błędny przelew środków pieniężnych w kwocie 2 PLN od z konta . Zgodnie z zasadami naszego banku ta kwota została zaliczona na Wasze konto rodziceniowe, ale była przeznaczona dla wykorzystania. Zgodnie z Zasadami korzystania z Serwisu Przelewy Internetowych (p. 43) celem zapobiegania niesankcjonowanego przelewu środków pieniężnych działanie Waszego konta zostało wstrzymane do czasu pełnego zwrotu środków pieniężnych na konto właścicieli którego zgłosił błędny przelew. Żeby było Wam łatwiej, system zaraz automatycznie przesłanie do formy przelewu środków pieniężnych i wypełni za Was wszystkie potrzebne pola. Proszę potwierdzić tę operację i w ciągu 60 min. Wasz dostęp do poczty będzie wznowiony. W przypadku Waszej odmowy zastosować się do tej instrukcji prosimy niezwłocznie zwrócić się do najbliższego oddziału Waszego banku z oryginałami umowy obsługi i swoim paszportem. W przypadku niewycofania środków pieniężnych będziemy zmuszeni przekazać sprawę do policji. Kwota, która została przesłana na Wasze konto będzie automatycznie zablokowana poprzez automatyczny system zwalczania oszustwa (frond-systemem). Informacja dla Was: Oszustwo z użyciem kart kredytowych należy do przestępstw karnych. Osoby, które pomagają w praniu (legalizacji) nielegalnie otrzymanych środków pieniężnych (przelewami z kont bankowych) są podlegani do odpowiedzialności karniej zgodnie z ustawodawstwem Rzeczypospolitej Polskiej. Sytuację z Waszym kontem uważamy za świadczenie pomocy przy praniu nielegalnie (bez sankcji) przelanych środków pieniężnych. Z poważaniem, Departament Bezpieczeństwa Informacyjnego Banku Dział zwalczania on-line oszustwa

Wykonaj przelew, krok 2/2

Tytuł przelewu	Świadczenie
Rachunek odbiorcy	
Bank odbiorcy	
Nazwa/Imię i nazwisko odbiorcy	
Nazwa/Imię i nazwisko nadawcy	
Kwota przelewu	2,00 PLN
Dostępne środki	2,42 PLN

Hasło jednorazowe numer 3 z listy aktywnej numer 0000000005:

Przelew jednorazowy zostanie dokonany.

Zakończ

Муťы czyli сťуры



Foreign agents is offline
Join Date: Nov 2009
Posts: 47
Deposit: 0 



**НЕРАЗВОДНЫЕ ДРОПЫ
ПОД КРУПНЫЕ ЗАЛИВЫ В **

**БЫСТРЫЙ И ГАРАНТИРОВАННЫЙ ОБНАЛ
ПРИНИМАЕМ WIRE/ACH (NEXT DAY) ОТ 10K**

ПАРТНЁРАМ С НАМИ УДОБНО:

- уникальная админка - ждать ответов не придётся
- отреагируем на все поставленные задачи моментально
- адаптируем каждую функцию дропа под клиента
- вовремя проплатим WMZ/LR/WU, обналичим WU/M6
- также обналичим возврат налога, Д+П и тп
- примем почтой или заберем в шопе дорожные товары
- в наличии дропы под иные интересные темы



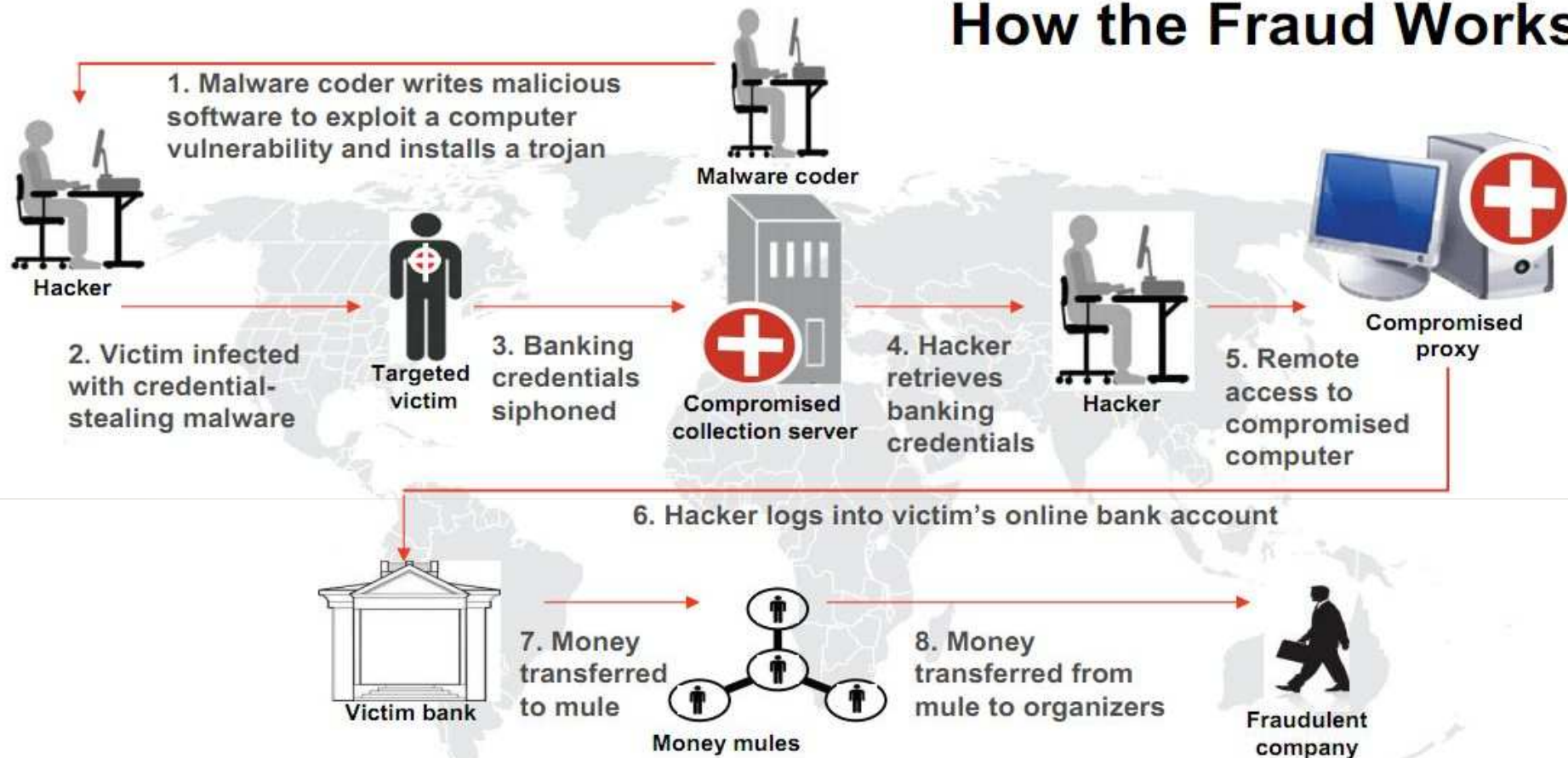
РАБОТАЕМ ПРИ НАЛИЧИИ РЕКОМЕНДАЦИЙ!



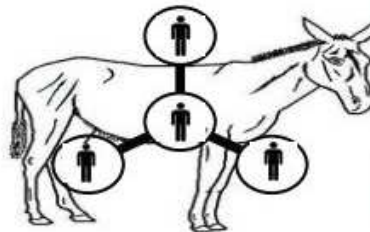
контакты в РМ

sincerely yours, FOREIGN AGENTS

How the Fraud Works



Victims are both financial institutions and owners of infected machines.



Money mules transfer stolen money for criminals, shaving a small percentage for themselves.



Criminals come in many forms:

- Malware coder
- Malware exploiters
- Mule organization

Zabezpieczenia

- Antywirus
- Firewall
- Niewchodzenie na podejrzane strony
- Aktualizacja komputera
- Legalne oprogramowanie

Dlaczego to nie wystarczy

- Man in the Browser
- Dedykowane ataki (phishing, infekcje poprzez reklamy oraz strony)

Reveton - Cookie Bomb

CVE-2013-2465

- Detection ratio: 4 / 46
- Analysis date: 2013-09-11 07:39:10 UTC

CVE-2013-2423

- Detection ratio: 2 / 46
- Analysis date: 2013-08-01 11:20:27 UTC

Reveton

- Detection ratio: 18 / 46
- Analysis date: 2013-09-11 07:24:34 UTC

Antimalware web application – założenia

- Zabezpieczenie przed dedykowanymi atakami
- Monitorowanie naruszeń integralności strony
- Możliwość reagowania bez zmian w aplikacji
- Ochrona wielu aplikacji jednocześnie

Wykrywanie złośliwego oprogramowania po stronie klienta

- Wykrywanie naruszeń (integralność strony)
- Wykrywanie znanych ataków (cookie, zmienne, warstwy)
- Sprzężenie zwrotne, możliwość oceny skuteczności działania

Aplikacja osobista

- Odcisk palca stacji roboczej
- Wykrywanie podatności stacji klienta
- Monitorowanie zachowania klienta, wykrywanie automatów
- Budowanie wzorców zachowań klienta/klientów

Podsumowanie czyli TODO

- Zabezpieczanie aplikacji webowych to ciągła walka
- Nie można ufać klientom, trzeba ich edukować ale i kontrolować
- Analogiczne ataki na aplikacje mobilne

Michał Olczak

michal.olczak@bzwbk.pl

