INCIDENT #74346

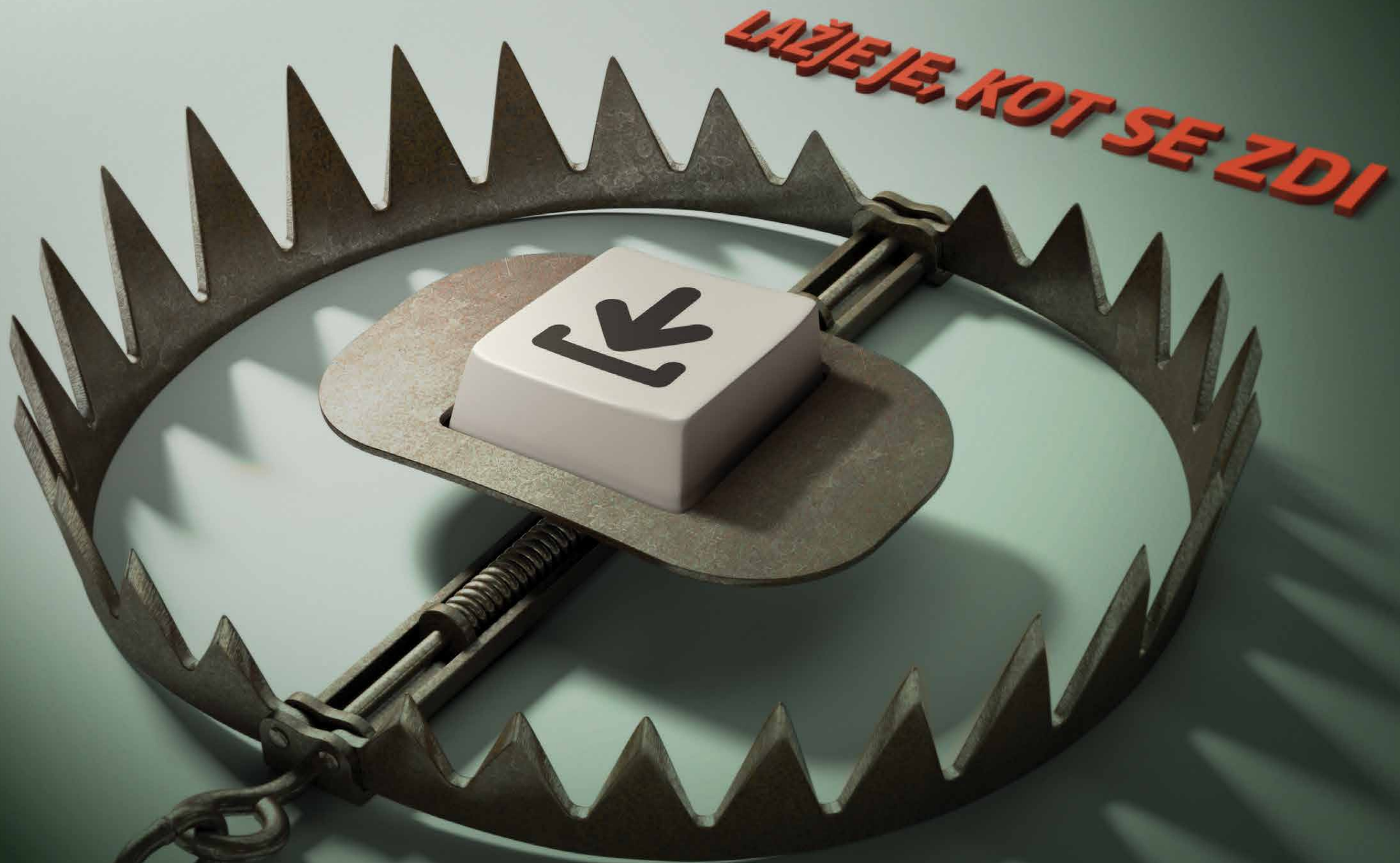
PHISHING SLOVENSKIH BANK

si·cert

gorazd.bozic@cert.si, @gbozic

POROČILO O OMREŽNI VARNOSTI ZA LETO 2014

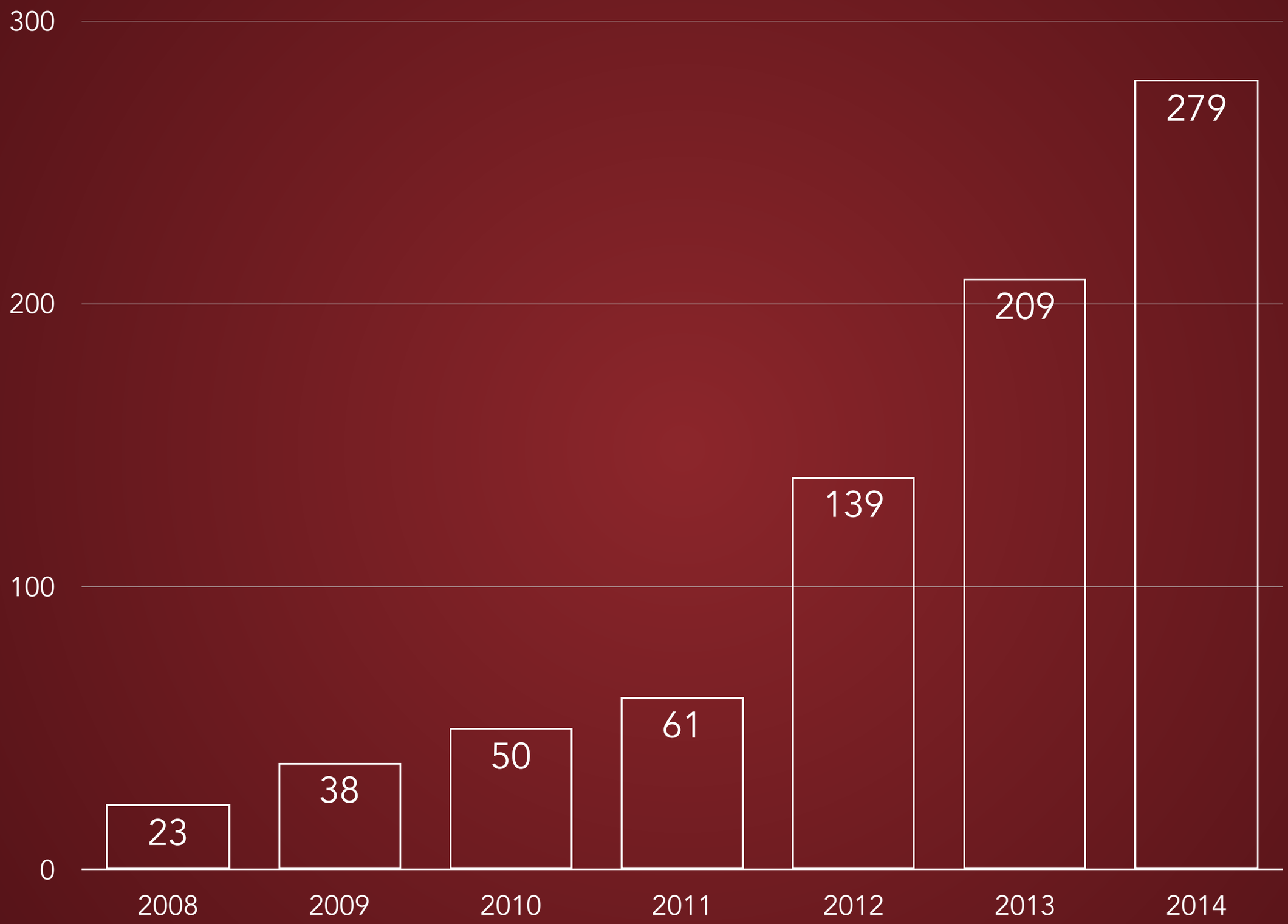
arnes si·cert VARNI NA INTERNETU



OTP

~

CERTIFIKAT


300
200
100
0
23
38
50
61
139
209
279
2008
2009
2010
2011
2012
2013
2014


User
Pass
Od skupno
279 phishing
napadov
jih je bilo
108 usmerjenih
na slovenske uporabnike,
171 pa podtaknjenih
spletnih strani
na slovenskih
strežnikih

NLB

SKB

SOCIETE GENERALE GROUP

ABANKA

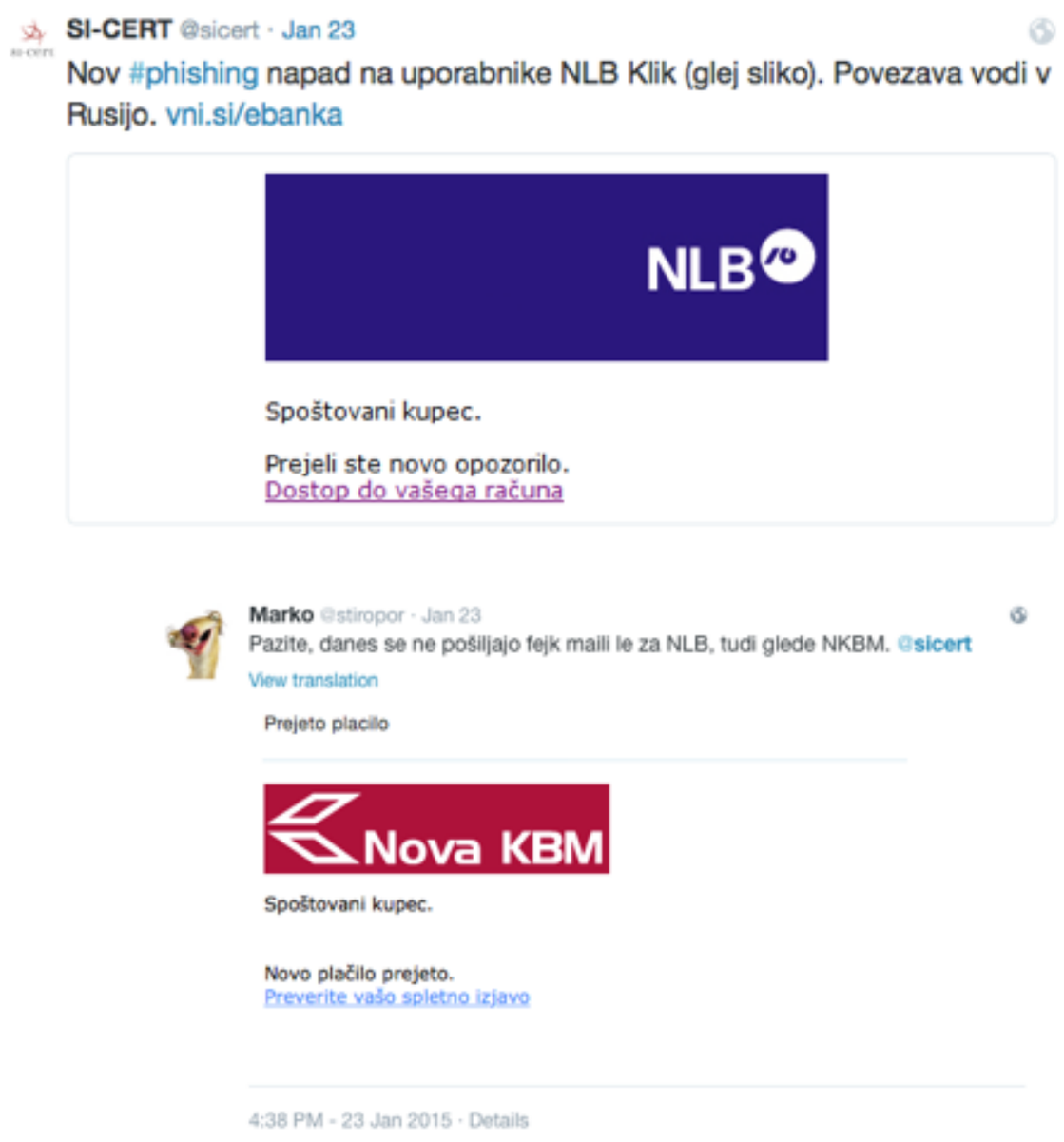
PROBANKA
finančna skupina

Nova KBM

UniCredit

PRVE PRIJAVE

- NLB, 23. 1. ob 11:53
- NKBM, 23. 1. ob 12:55
- zatišje čez vikend
- NKBM, 26. 1. ob 09:52



< Nova

To: [redacted]

Sporocilo #96389711

Spoštovani kupec.

Vaš račun zahteva dodatno preverjanje.
Kliknite tukaj za Ravnati

http://pilateszone.com.br/dd/

Nova KBM

To: [redacted]

Obvestilo

Spoštovani kupec.

Prejeli ste novo varnostno opozorilo.
Dostop do vašega računa

http://yaktash.ru/aq/

Nova Bank@Net

To: [redacted]

Obvestilo

Spoštovani kupec.

Vaš račun zahteva dodatno preverjanje.
Kliknite tukaj, da začnete preverjanje.

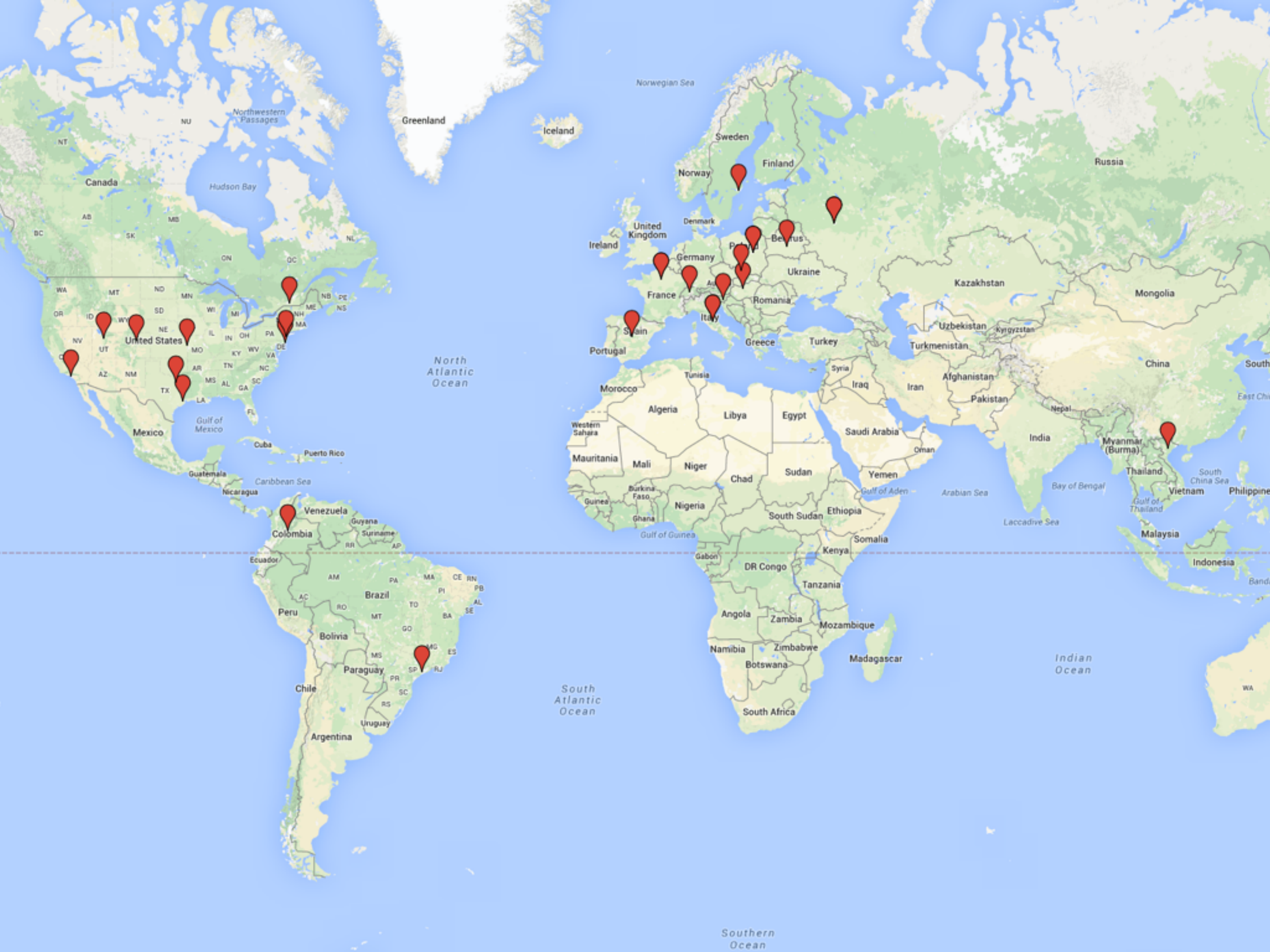
http://healthywhey.ca/dir/

http://kominsystem.pl/nk/
http://neoubeauty.vn/op/
http://yaktash.ru/aq/
http://launchmd.com/si/
http://pfshop.ru/sk/
http://wiki.imz-medizinzentrum.de/a/
http://consorziomoscatodiscanzo.it/www2/
http://www.ppcss.fr/sp/
http://www.elmax-wloszczowa.pl/wp-content/si/
http://www.cvtslandscape.com/si/
http://www.hospitaloccidentekennedy.gov.co/si/
http://velta.hu/banknet/nkbm/
http://rumoro.by/banknet/nkbm/
http://www.itum.com.pl/banknet2/
http://biztraining.sg/si/
http://maniosdigital.com/si/
http://intersismet.com/si/
http://www.pourlespme.com/si/
http://pilateszone.com.br/dd/
http://troi-food.ch/scripts/uploadify/si/
http://www.uesants.cat/si/
http://yahvi.org/si/

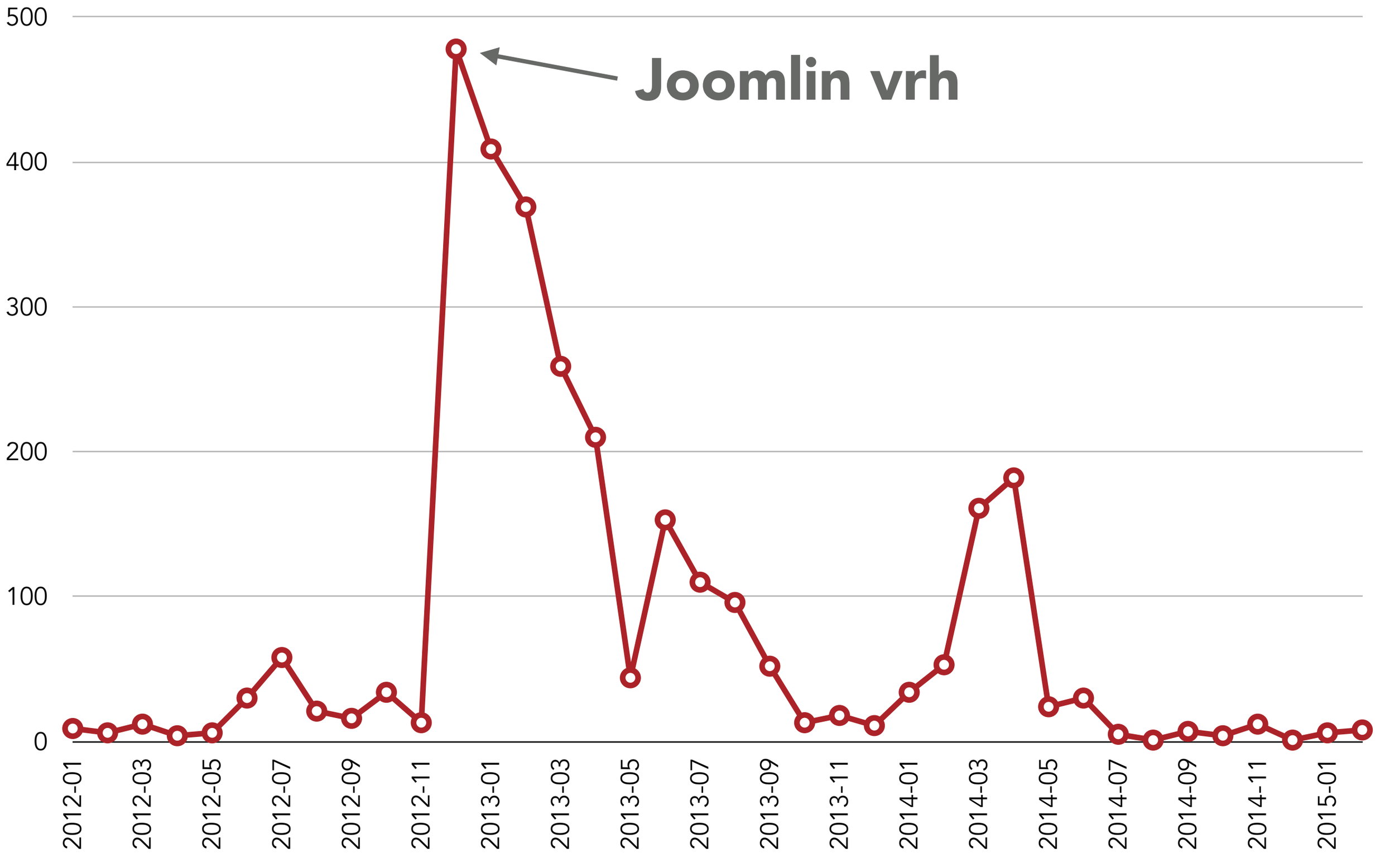
redirect

http://themovieforum.org/banknet/
http://pfshop.ru/banknet/
http://www.osni.fr/banknet/
http://www.osni.fr/klikotp/nlb/si/login3.html
http://www.osni.fr/splet/probanka.si/pls/login3.html
http://hudkliniken.com/banknet/
http://yousol.com.br/banknet/
http://www.poweradvisoryllc.com/banknet/
http://paletsmadrid.com/banknet/nkbm/prijava/login2.html
http://mishtal.ru/si/
http://www.wyroki.eu/si/skb.net/Default/login2.html
http://www.wyroki.eu/epoti/

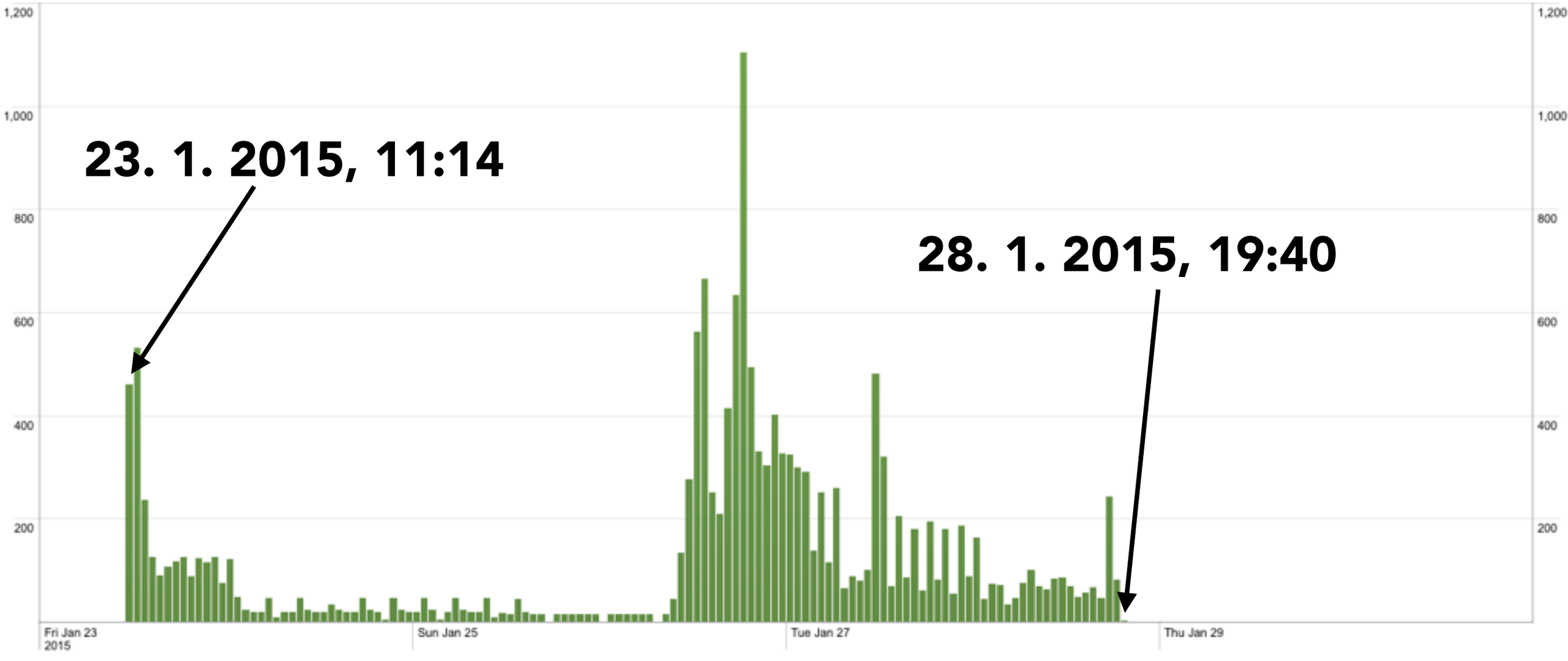
landing


Greenland
Iceland
Norwegian Sea
Northwestern Passages
Hudson Bay
Canada
NU
NT
AB
BC
SK
MB
ON
QC
NL
NB
PE
NS
ME
NH
MA
DE
WA
MT
ND
MN
OR
ID
SD
WI
MI
WY
NE
IL
IN
OH
PA
NV
UT
CO
MO
KY
WV
VA
AZ
NM
AR
TN
NC
MS
AL
GA
SC
TX
LA
FL
United States
Gulf of Mexico
Mexico
Cuba
Puerto Rico
Caribbean Sea
Guatemala
Nicaragua
North Atlantic Ocean
Sweden
Finland
Norway
Russia
Denmark
United Kingdom
Ireland
Germany
Belarus
Ukraine
France
Romania
Italy
Spain
Portugal
Greece
Turkey
Kazakhstan
Mongolia
Uzbekistan
Kyrgyzstan
Turkmenistan
China
Afghanistan
Iran
Iraq
Syria
Pakistan
Nepal
India
Saudi Arabia
Oman
Yemen
Gulf of Aden
Arabian Sea
Bay of Bengal
Myanmar (Burma)
Thailand
Vietnam
Malaysia
Indonesia
South China Sea
Gulf of Thailand
Laccadive Sea
Tunisia
Morocco
Algeria
Libya
Egypt
Western Sahara
Mauritania
Mali
Niger
Chad
Sudan
Burkina Faso
Guinea
Nigeria
Ghana
Gulf of Guinea
South Sudan
Ethiopia
Somalia
Kenya
Gabon
DR Congo
Tanzania
Angola
Zambia
Mozambique
Namibia
Zimbabwe
Botswana
Madagascar
South Africa
Indian Ocean
Venezuela
Colombia
Guyana
Suriname
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Argentina
Uruguay
South Atlantic Ocean
Southern Ocean

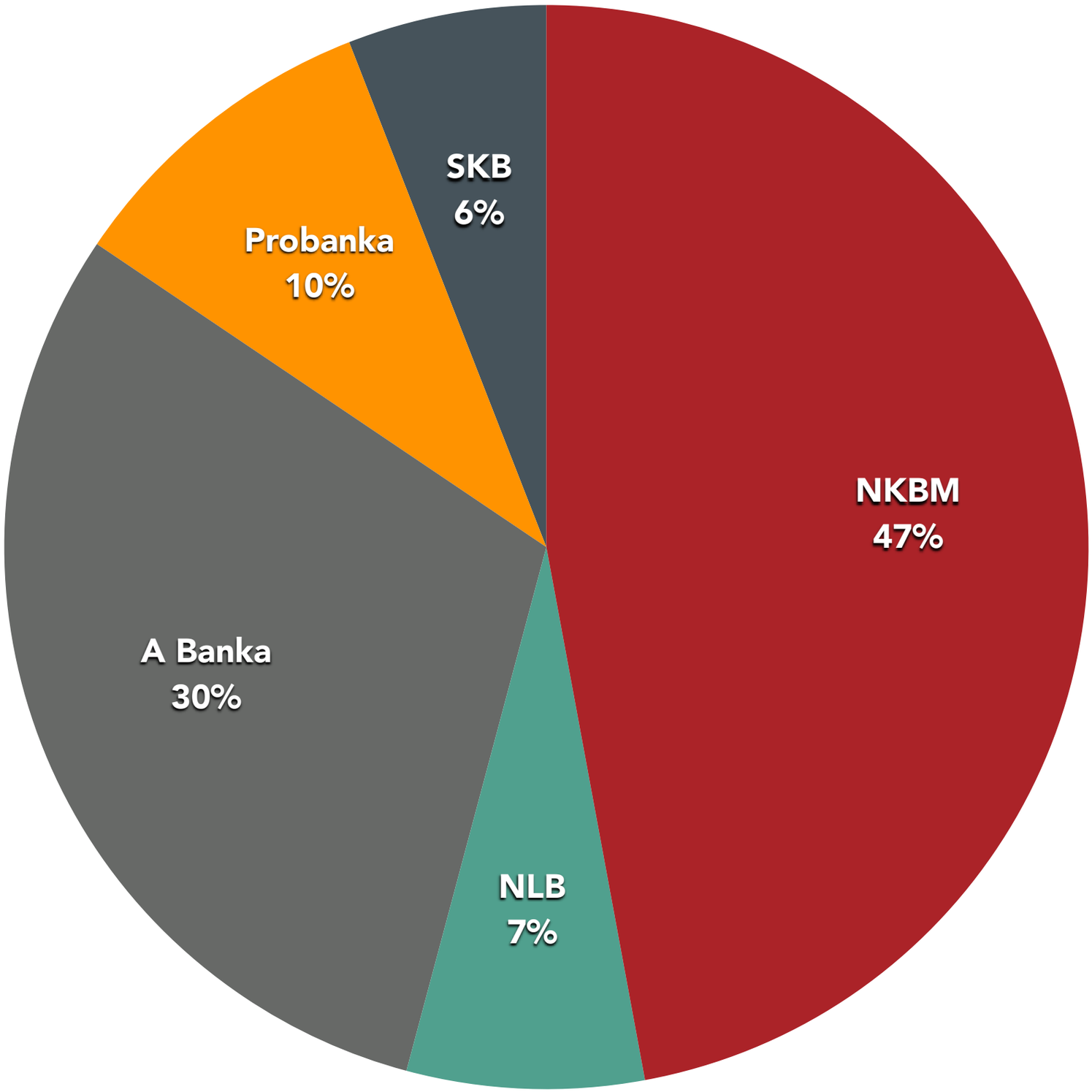
RAZOBLIČENJA NA MESEC

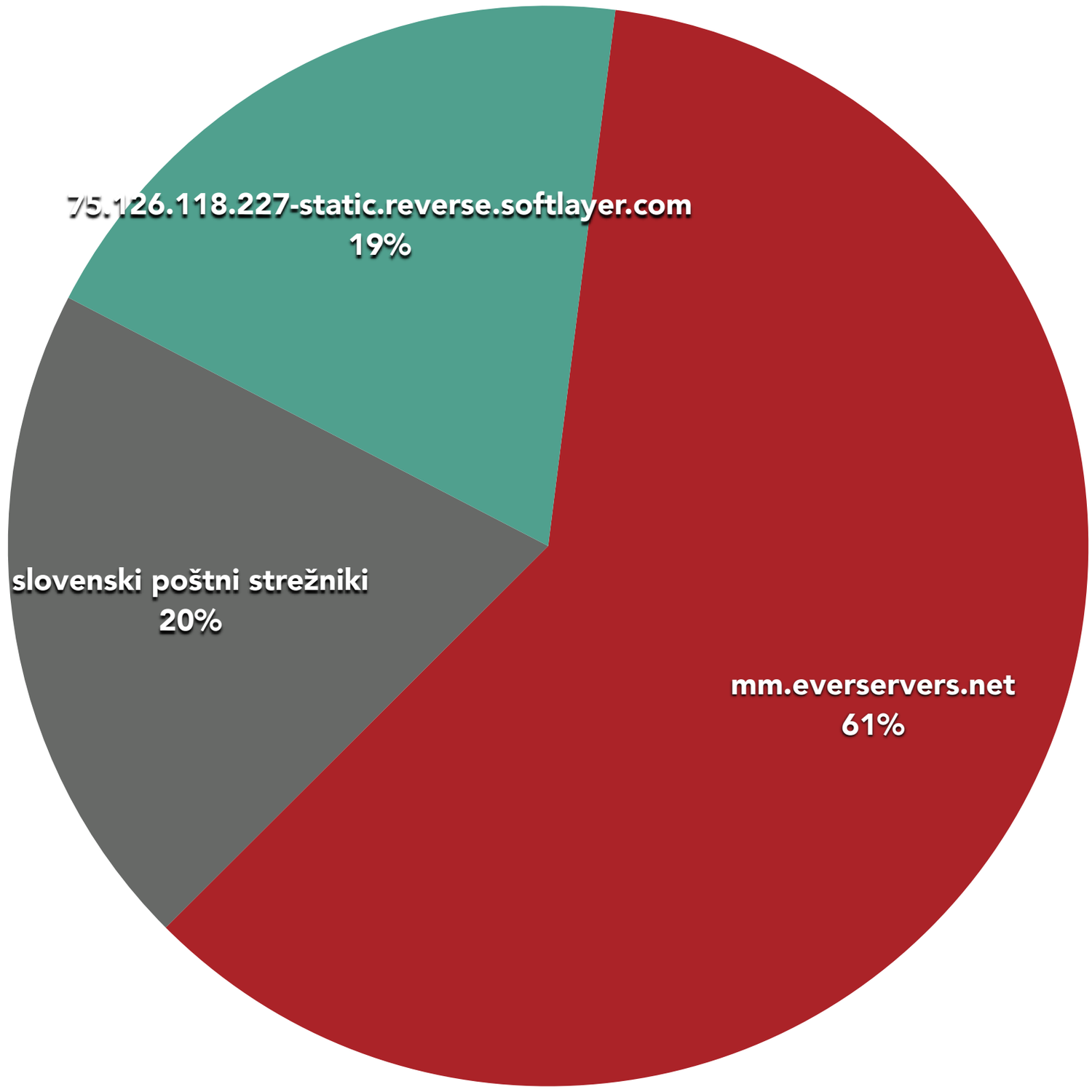


rejected:
(kbm@nova-kbms.si OR klikotp@nlbklik.si OR localhost@everservers.net OR localhost@sites2sl.sageisland.com OR noreply@abanka-net.si OR noreply@novakbms.si OR noreply@novakbms1.si OR payment@probankasi.si OR pm@skbindex.si OR pt@novakmbsi.si) NOT "-bounces"



15446 sporočil


SKB
6%
Probanka
10%
NKBM
47%
A Banka
30%
NLB
7%


75.126.118.227-static.reverse.softlayer.com
19%
slovenski poštni strežniki
20%
mm.everservers.net
61%

PONUDNIKI

- obvestilo članom SIX
- obvestilo registrarjem - ponudnikom gostovanja

TAKEDOWN

CERT-GIB Incident Response Team
To: Si-CERT
[Ticket#2015012710000197] RE: [SI-CERT #74455] Urgent: Phishing web si [...]

[An English message follows below]

Здравствуйте,

CERT-GIB благодарит Вас за обращение.

Номер Вашей заявки 2015012710000197.

Пожалуйста используйте этот номер в дальнейшем для связи с нами по данному инциденту.

Обращаем Ваше внимание на то, что все заявки регистрируются и обрабатываются в порядке поступления.
Мы приступим к решению Вашего вопроса максимально оперативно и оповестим Вас как только он будет решен.

При необходимости наш сотрудник может связаться с Вами дополнительно.

В случае, если Ваша проблема является срочной и требует незамедлительного решения, просим Вас связаться с нами по телефону +7 (495) 984 33-64.

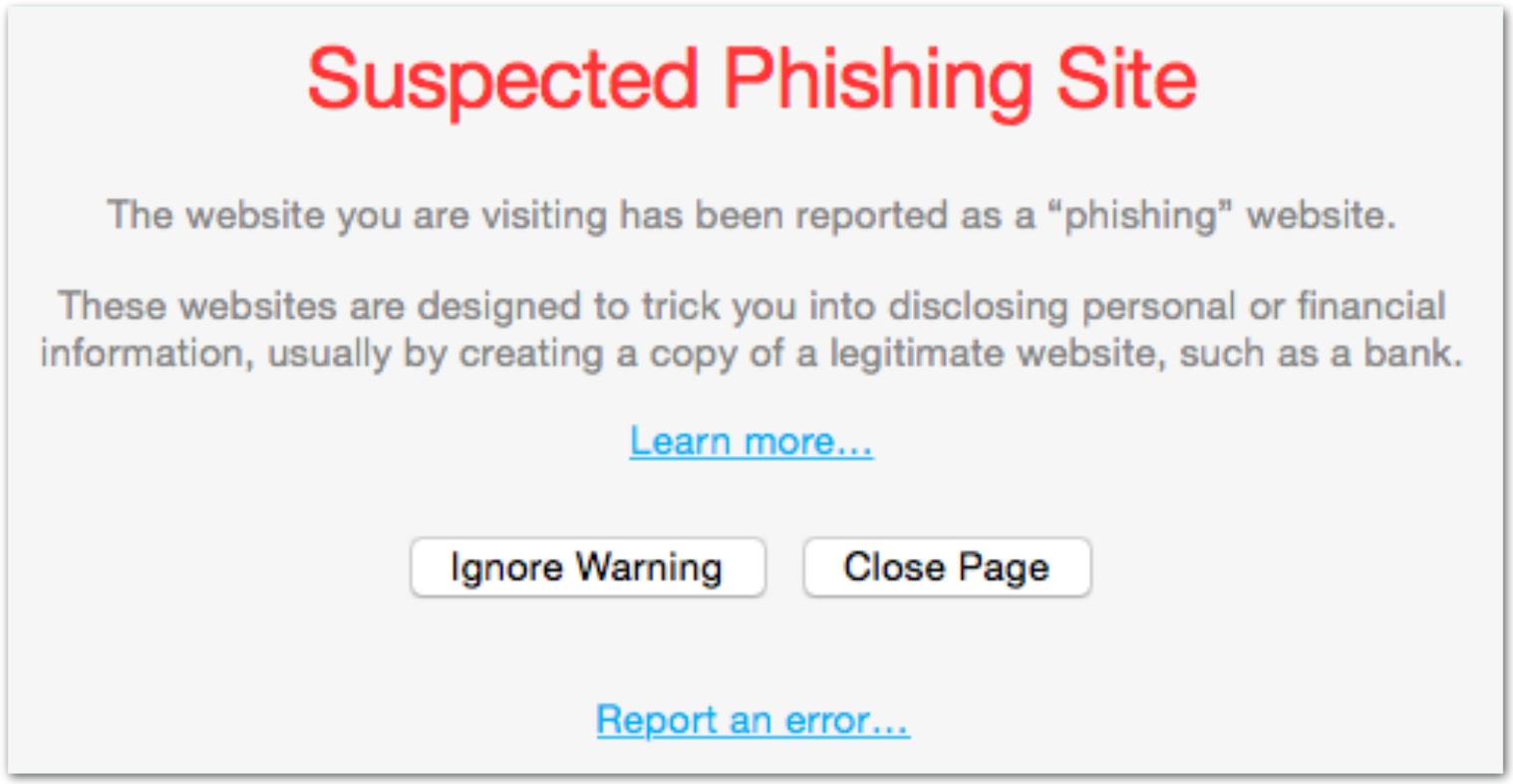
Это сообщение было создано автоматически. Мы заинтересованы в оперативном разрешении Вашей проблемы.
Пожалуйста, не создавайте дополнительных заявок по данному инциденту – это замедлит обработку уже полученной заявки!

С уважением,
CERT-GIB
+7 (495) 984 33-64
response@cert-gib.ru
http://www.cert-gib.ru

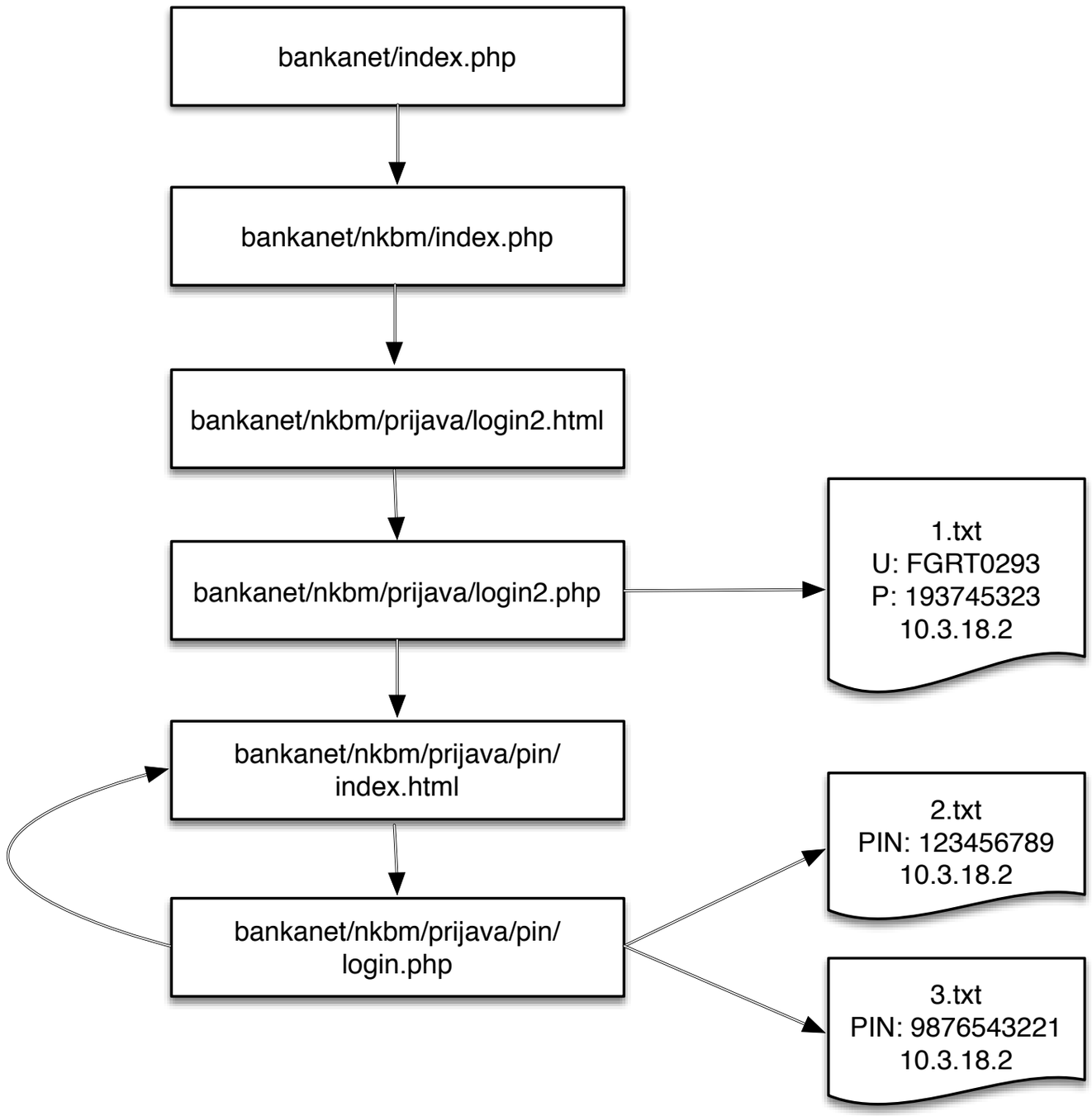
Ошибка 502

Сервер не отвечает. Пожалуйста, повторите запрос через некоторое время.

SEZNAMI ZA VARNO BRSKANJE



bankanet.zip



```php
<?php
include 'random.php';
?>
<html>
<script language="javascript">
var page = "prijava/login2.html?<?php echo $randomise; ?>" //the page to redirect.
top.location = page;
</script>
</html>
```

```php
<?php
/// TIME
date_default_timezone_set('GMT');
$TIME = date("d-m-Y H:i:s");

/// COUNTRY
$PP = getenv("REMOTE_ADDR");
$J7 = simplexml_load_file("http://www.geoplugin.net/xml.gp?ip=$PP");
$COUNTRY = $J7->geoplugin_countryName ; // Country

/// VISITOR
$ip = getenv("REMOTE_ADDR");
$file = fopen("../visit.txt","a");
fwrite($file,$ip."  -   ".$TIME."                    -        " . $COUNTRY ."\n")  ;

/// RANDOM
$one = rand(10,1000000) . rand(10,100000);
$length = 100;
$two = substr(str_shuffle("0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"), 0, $length);
function tree($length = 100) {
    return substr(str_shuffle("0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"), 0, $length);
}
$randomise = tree() . $two . $one;
?>
```

MEDIJI

PREVIDNO

Pazite na bančne račune: Slovenija tarča najbolj množičnega napada

Objavljeno: 27.01.2015 21:30 Posodobljeno: 27.01.2015 21:31

Avtor: A. L., T. L.

Ključne besede: NKBM, goljufija, spletna banka, Bank@Net, spletno ribarjenje, zvabljanje, phishing

Tarče napada so komitenti Nove Ljubljanske banke (NLB), Nove Kreditne banke Maribor (NKBM), SKB banke, Abanke, Unicredit banke in Probanke.

U: JKTR■■■■
T: 8245987678
193.201.■■.■■

U: ROHU■■■■
T: 1111878556
193.201.■■.■■

U: MAKO■■■■
T: 5123320880
86.58.■■.■■

U: ROHU■■■■
T: 1111474096
193.201.■■.■■

U: ROHU■■■■
T: 1111996215
193.201.■■.■■

U:
T:
80.82.■■.■■

U: fuckyou
T: 1541214752
90.157.■■.■■

U: sdfsd
T: sdfsddde33
64.122.■■.■■

U: umbar
T: 1234567890
94.103.■■.■■

U: kreten
T: 1234567890
94.103.■■.■■

U: idiot
T: 0987654321
94.103.■■.■■

SI-CERT @sicert · Jan 27

Vsem, ki nam posredujete phishing sporočila, se lepo zahvaljujemo. Trenutno smo preobremenjeni, da bi se lahko zahvalili vsakemu posebej.

2 2

SI-CERT @sicert · Jan 26

Poteka najbolj množičen in sofisticiran #phishing napad v Sloveniji. Zaenkrat tarča 5 bank, pričakujemo jih še več: cert.si/si-cert-2015-0…

69 13

SI-CERT @sicert · Jan 26

SI-CERT 2015-01 / Val phishing napadov na slovenske banke cert.si/si-cert-2015-01

5

SI-CERT @sicert · Jan 26

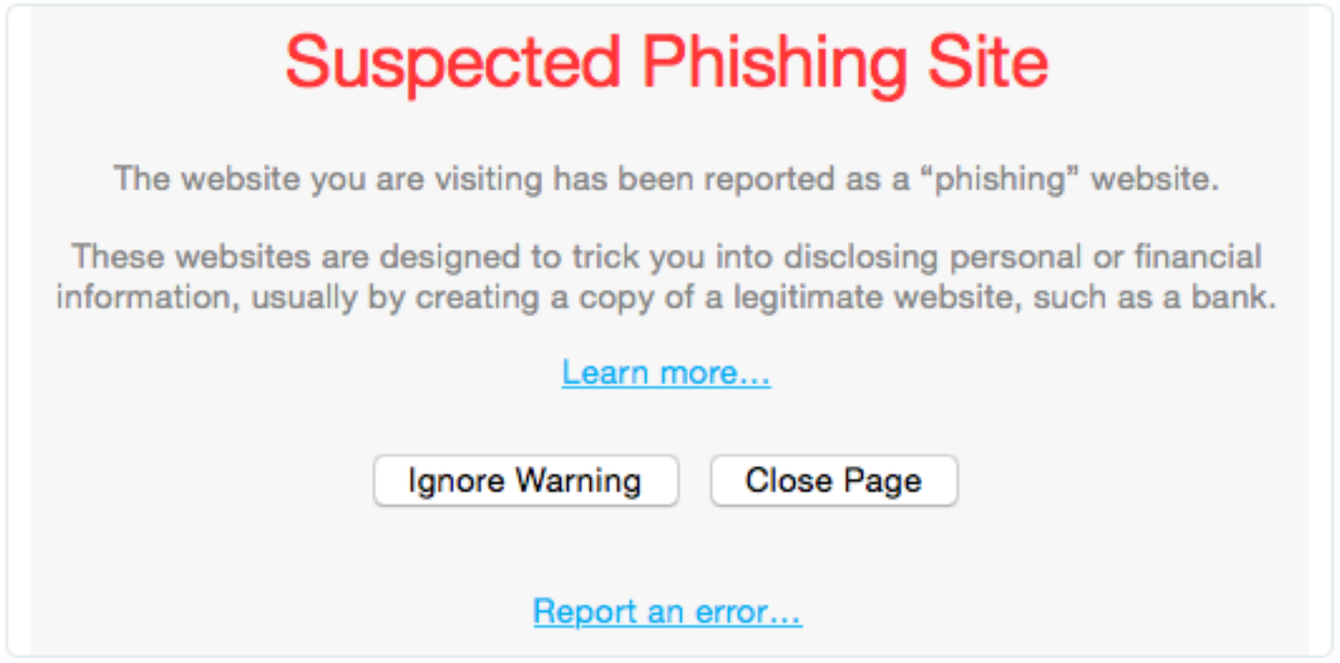
.@blazoncek Ravnokar prejeli obvestilo tudi o tem. Prosimo za posredovanje sporočil na cert@cert.si. Hvala! @pu7r

3

View conversation

SI-CERT @sicert · Jan 28

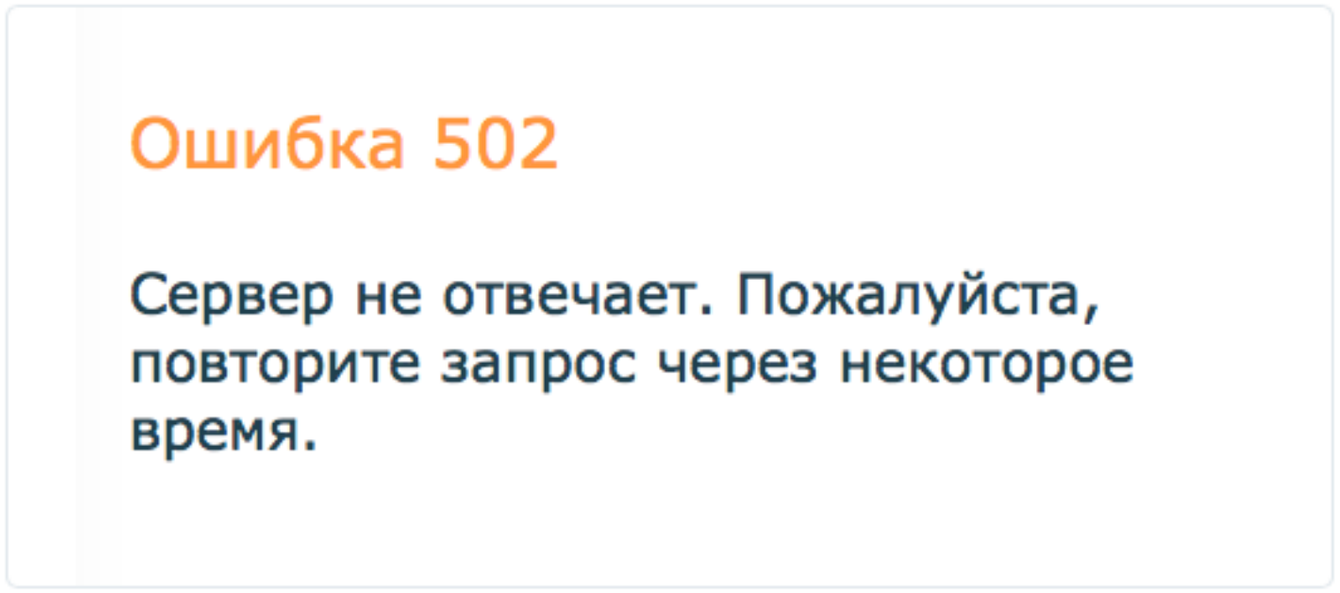
Vse naslove smo spravili tudi na sezname sumljivih spletnih strani, ki jih uporabljajo brskalniki. #phishing 2/4



3 3 View more photos and videos

SI-CERT @sicert · Jan 28

Odstranjene so vse #phishing spletne strani za slovenske banke, tako tudi skoraj vse preusmeritve. 1/4



4 2 View more photos and videos

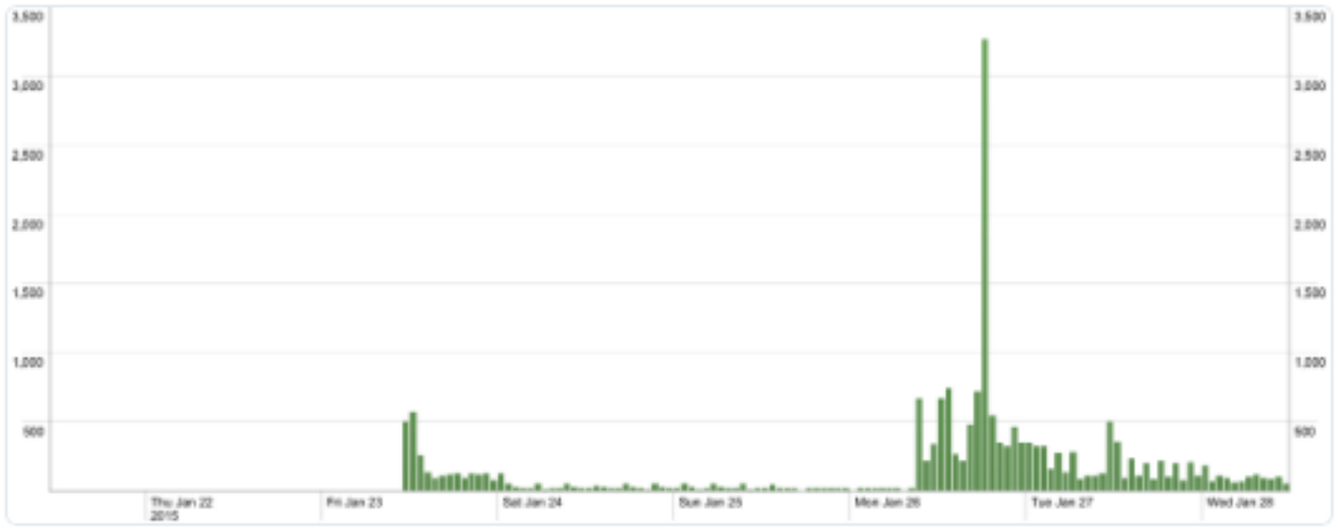
SI-CERT @sicert · Jan 28

Vsem, ki ste nam te dni posredovali #phishing sporočila, se zahvaljujemo. Pomagali ste nam identificirati vedno nove spletne lokacije. 4/4

2 2

SI-CERT @sicert · Jan 28

Tudi graf zavrnjenih #phishing sporočil kaže na konec tega vala napada na 6 slovenskih bank. 3/4



5 2

View more photos and videos

INCIDENT #74346

- 84 prijav
- 42 preiskav
- 22 preusmeritvenih naslovov
- 12 “pristajalnih” mest

NASLEDNJIČ

- škodljiva koda
- prestrezanje SMS sporočil
- proxy infrastruktura
- DNS preusmeritve

REZULTATI

- izboljšani odnosi z bankami in ZBS
- sestanek na GPU MNZ
- dopolnjeni interni postopki

OPAŽANJA

- dober odziv uporabnikov (=prijave)
- stalno delovanje moti storilce
- **nekateri ponudniki odreagirali**
- **spam blokiranje preko postmastrov**
- **.ru in .by presenetila (.fr razočaral)**