

CONFERENCE

# ZERONIGHTS 2014

NOVEMBER 13-14

Roaming tiger

Anton Cherepanov

cherepanov@eset.sk



ENJOY SAFER TECHNOLOGY™



[WWW.ZERONIGHTS.ORG](http://WWW.ZERONIGHTS.ORG)

In 2014 ESET observed similar attacks in Russia and CIS countries: Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Ukraine and Uzbekistan

### Similarities:

- Same infection vectors
- Use of RTF exploits since autumn of 2014
- Same malware families are used in attacks
- Purpose is to steal data



## Characteristics of “Roaming tiger”:

- High profile victims in Russia
- Use of RTF vulnerabilities (CVE-2012-0158 and CVE-2014-1761)
- Win32/Korplug (aka PlugX RAT)
- Win32/Farfli.BEK (aka Gh0st RAT)

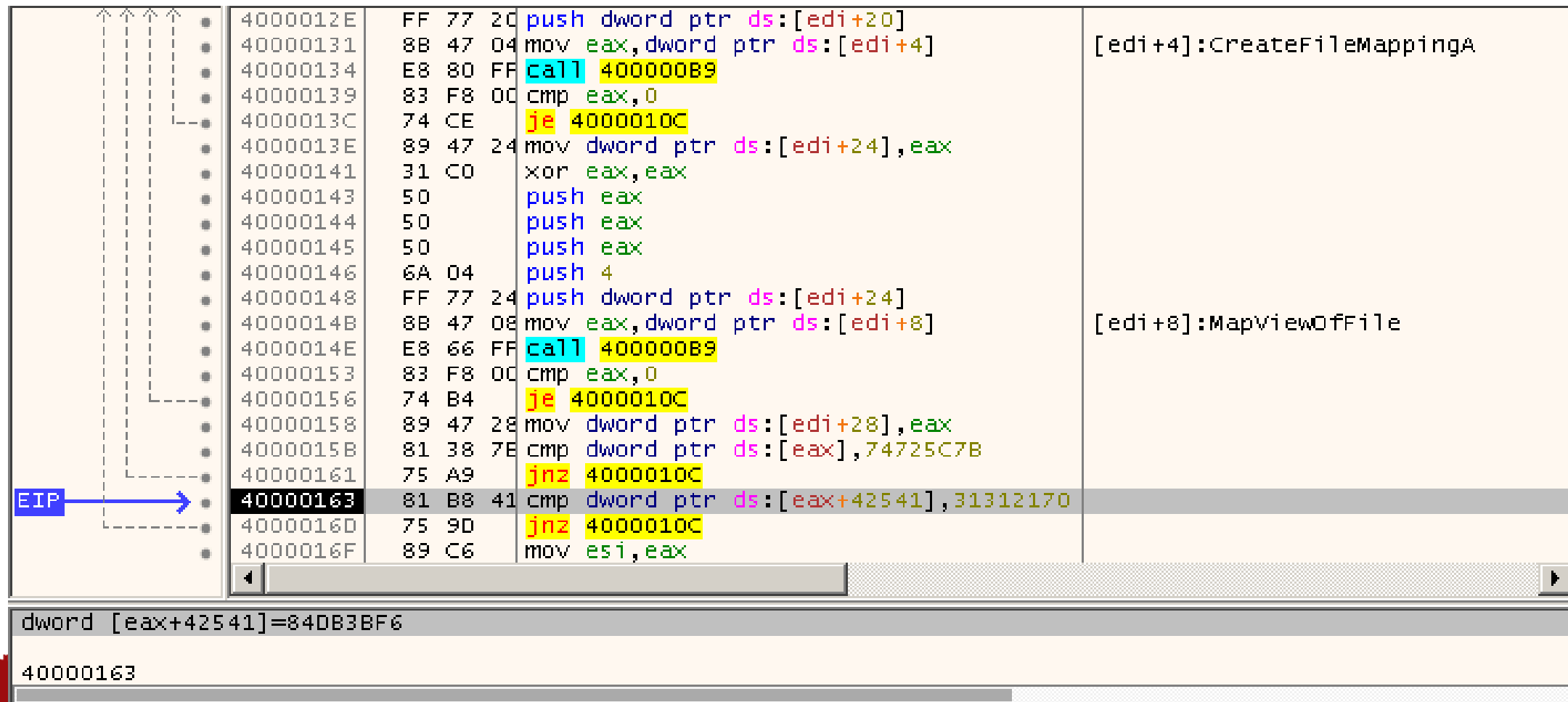


# CVE-2014-1761 copied from the same template:

```
1498 }}{\0007a0e83d86807ae600f71e08f356504add484a9f2c2620832c74a302fcf66b0073dca471d2
ccc6\000000000000000000000000027ae00000000d200e4ded8d2ba713b2dba71a68a9cbee4395
f85064c789000001ea43f000000e0486d\listoverride\000000000000000000254300000000
000e75e280e02041ce4eccdfae3e00f2fef6eb8cf7e5b5\bf999e8e23797d7a7c534640135a5e2b
253e237d010c4f070eefa7e4fdb9dbeaf891dad2a7ace1d8\ae0000000d200e4ded8d2ba713b2db
a71a68a9cbee4395f85064c789000001ea43f000000e0486d\listoverridecount000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000270d0a00e4ded8d2ba7
13b2dba71a68a9cbee4395f85064c789000001ea43f000000e0486d\25\6b7042f300a00000587dd
b4b3114172ed78d68b5cbf1707523059ae89cde005f3cb4c6463d5fd49d
1499 {\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\l
folevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfole
evel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfolevel}\lfoleve
l}\lfolevel}\lfolevel}\lfolevel}\lfolevel}
1500 {\lfolevel\listoverridestartat\listoverrideformat{\listlevel\levelnfc0\levelnfcn
249\leveljcn0\leveljcn0\levelfollow39\levelstartat31611\levellegal1\levelnrestart
0\levelpicture1\levelold0\levelprev1\levelprevspace1\levelspace22873\levelindent
23130}}
```



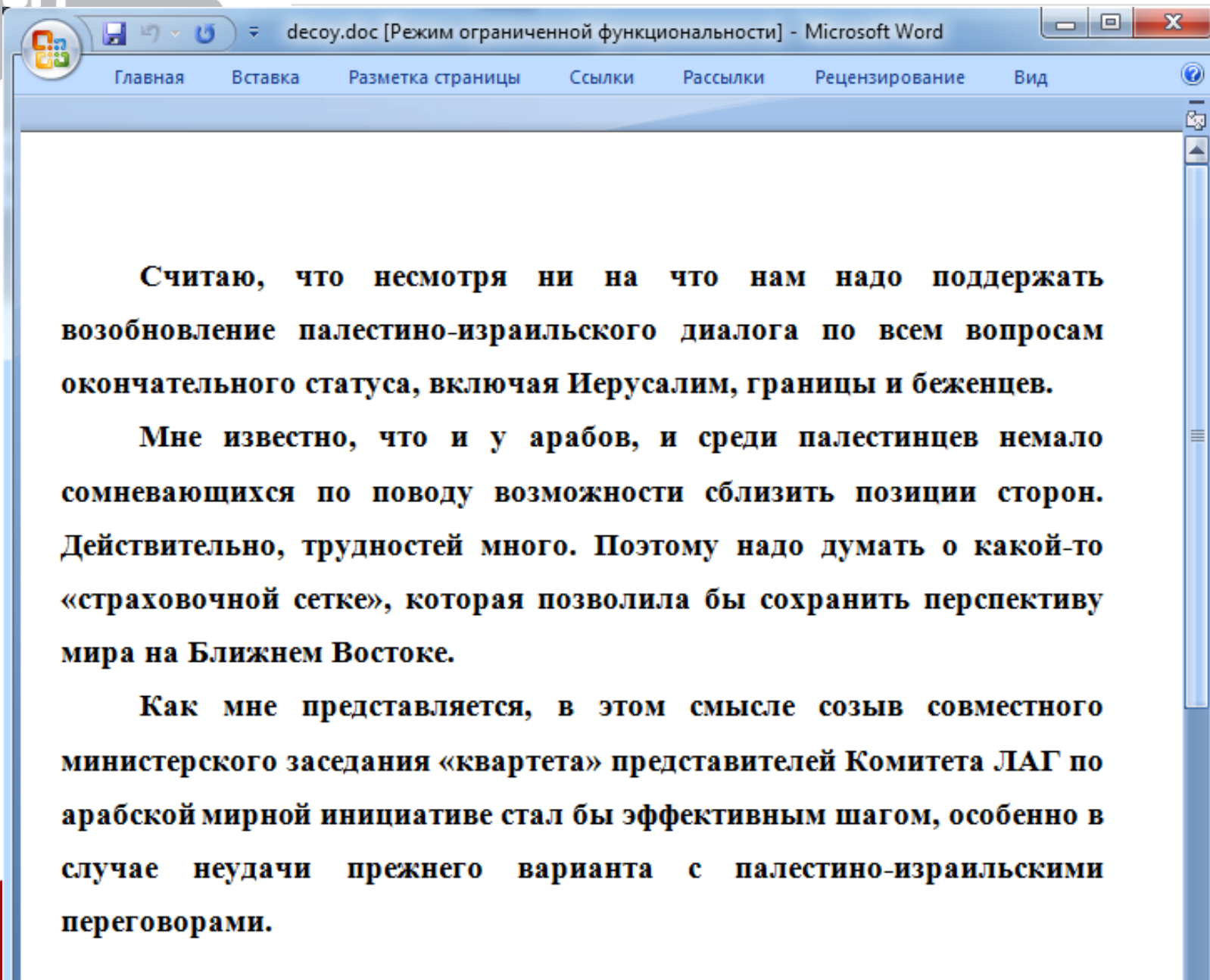
## First stage shellcode can't find second stage shellcode "p!11"-marker:

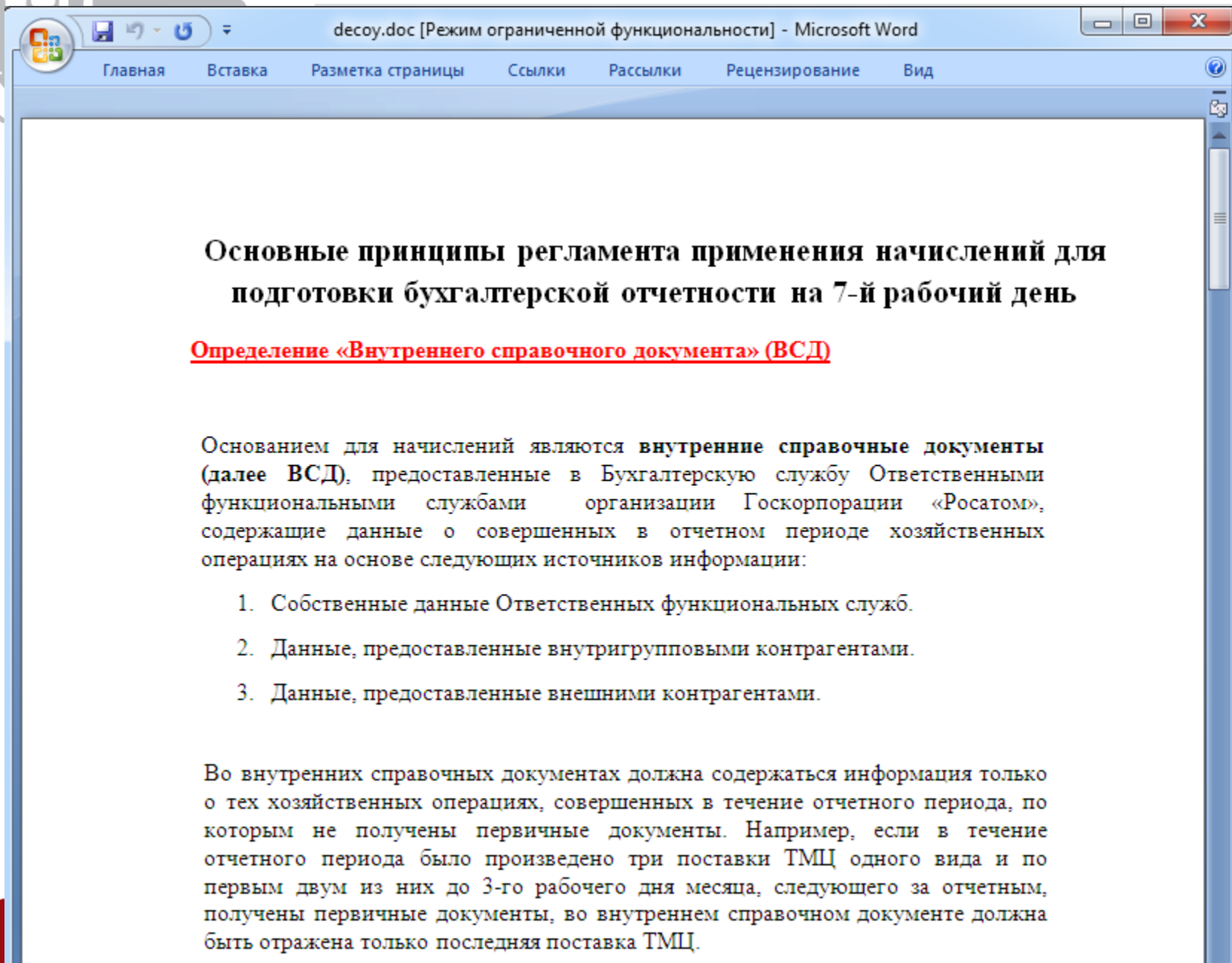


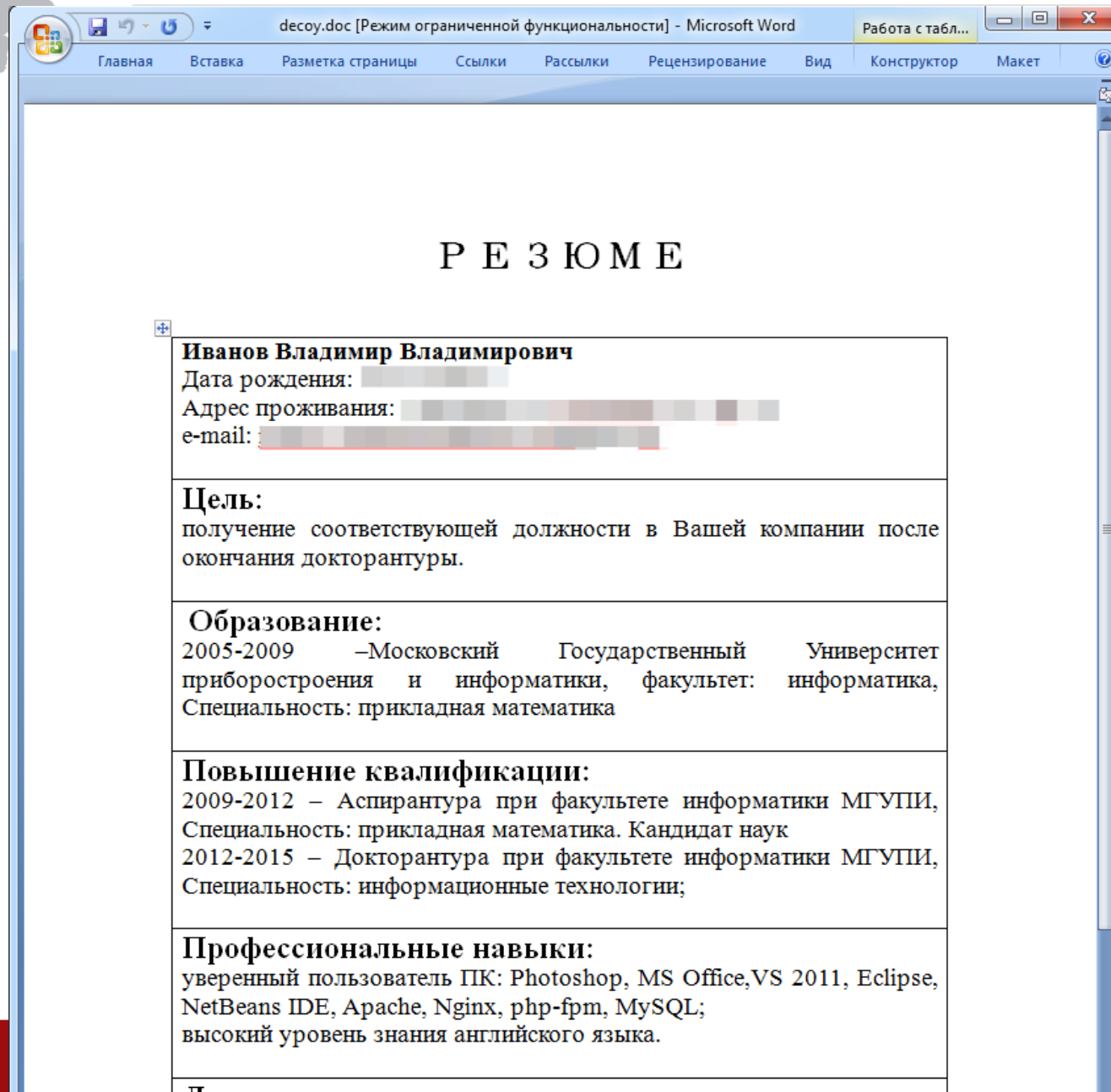
4000012E	FF 77 20	push dword ptr ds:[edi+20]	
40000131	8B 47 04	mov eax,dword ptr ds:[edi+4]	[edi+4]:CreateFileMappingA
40000134	E8 80 FF	call 400000B9	
40000139	83 F8 00	cmp eax,0	
4000013C	74 CE	je 4000010C	
4000013E	89 47 24	mov dword ptr ds:[edi+24],eax	
40000141	31 C0	xor eax,eax	
40000143	50	push eax	
40000144	50	push eax	
40000145	50	push eax	
40000146	6A 04	push 4	
40000148	FF 77 24	push dword ptr ds:[edi+24]	
4000014B	8B 47 08	mov eax,dword ptr ds:[edi+8]	[edi+8]:MapViewOfFile
4000014E	E8 66 FF	call 400000B9	
40000153	83 F8 00	cmp eax,0	
40000156	74 B4	je 4000010C	
40000158	89 47 28	mov dword ptr ds:[edi+28],eax	
4000015B	81 38 7E	cmp dword ptr ds:[eax],74725C7B	
40000161	75 A9	jnz 4000010C	
40000163	81 B8 41	cmp dword ptr ds:[eax+42541],31312170	
4000016D	75 9D	jnz 4000010C	
4000016F	89 C6	mov esi,eax	

dword [eax+42541]=84DB3BF6

40000163



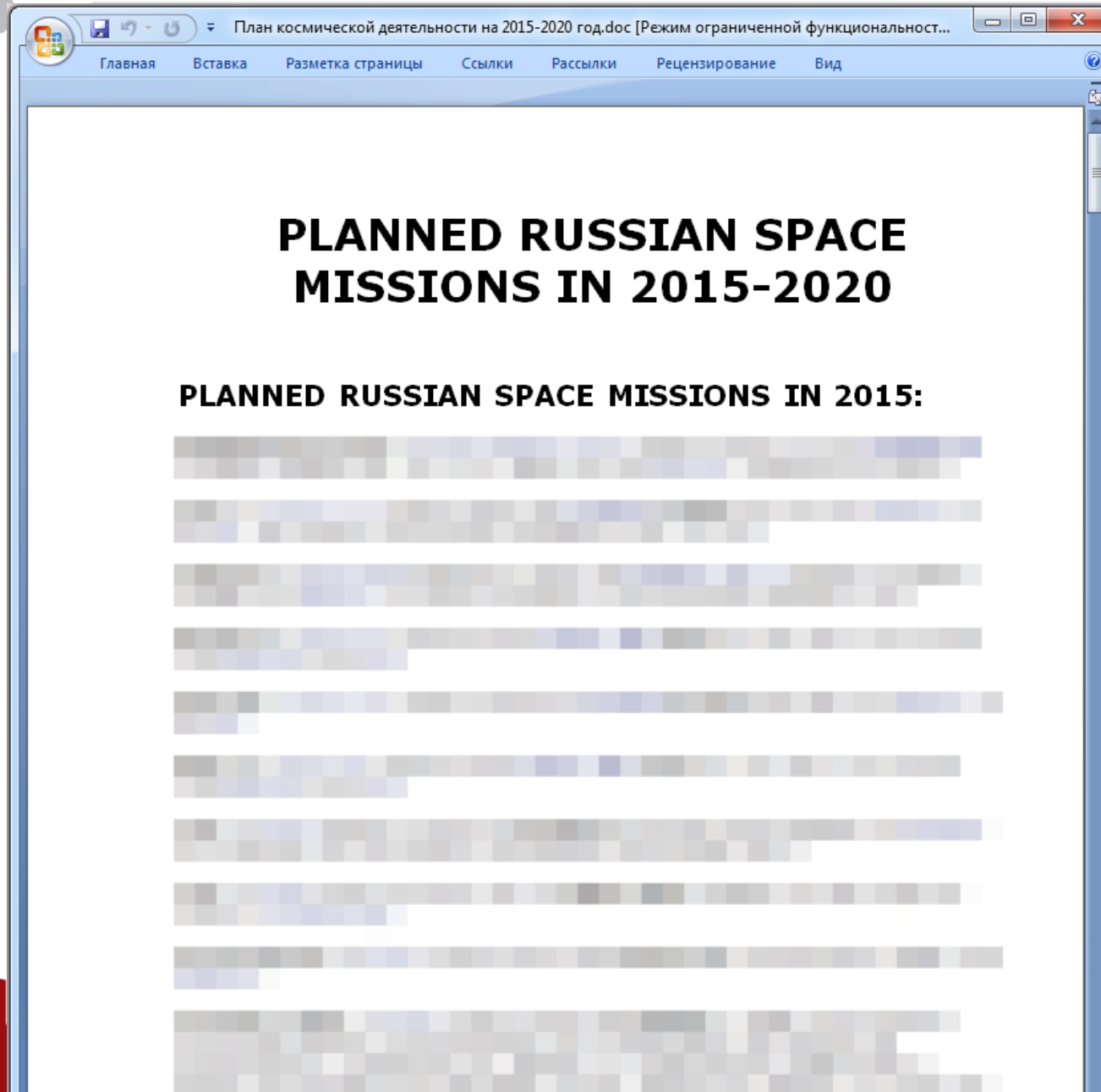


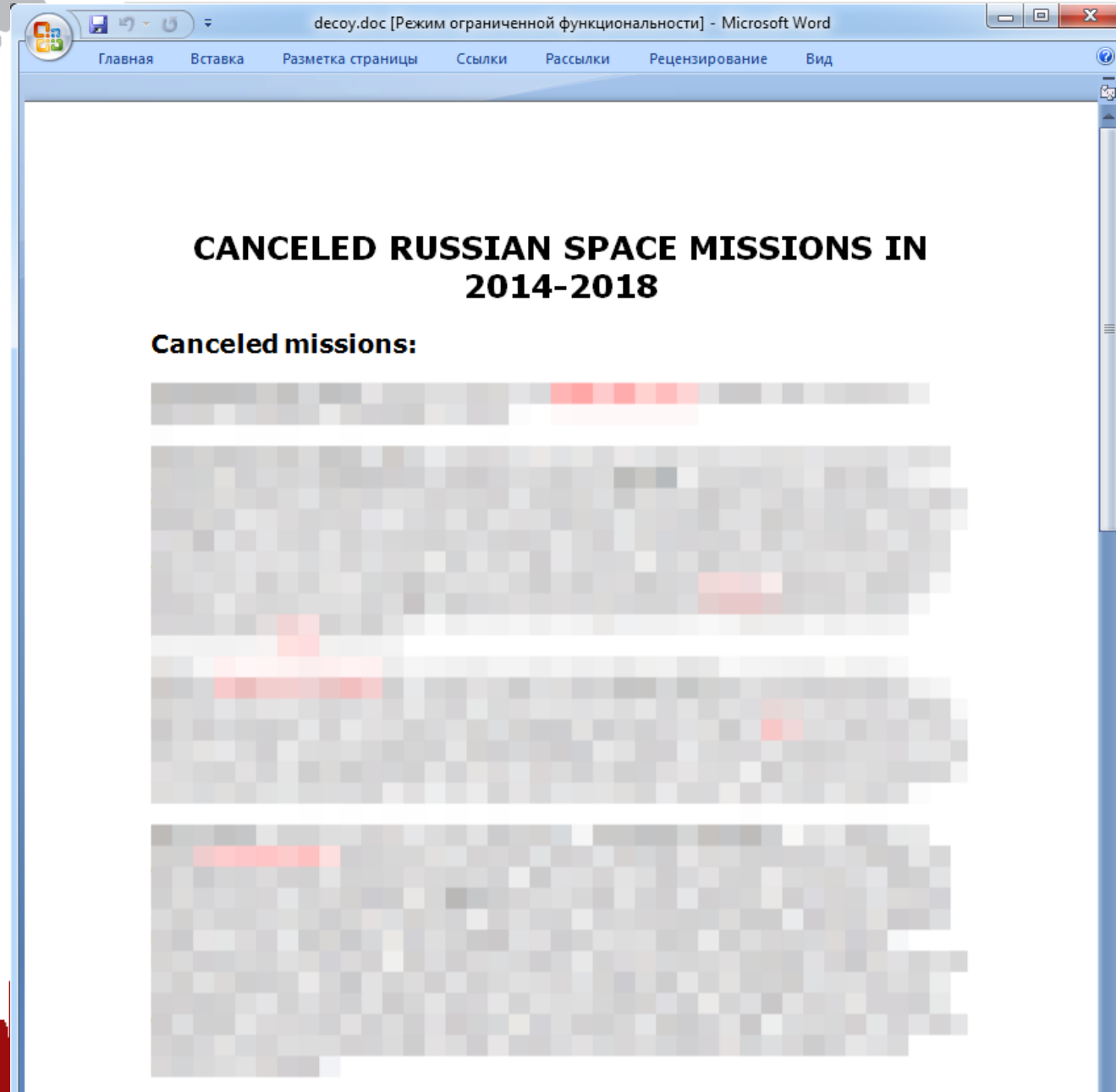


The screenshot shows a Microsoft Word window titled 'decoy.doc [Режим ограниченной функциональности] - Microsoft Word'. The ribbon includes 'Главная', 'Вставка', 'Разметка страницы', 'Ссылки', 'Рассылки', 'Рецензирование', 'Вид', 'Конструктор', and 'Макет'. The document content is a resume for Vladimir Vladimirovich Ivanov.

<b>Иванов Владимир Владимирович</b> Дата рождения: [REDACTED] Адрес проживания: [REDACTED] e-mail: [REDACTED]
<b>Цель:</b> получение соответствующей должности в Вашей компании после окончания докторантуры.
<b>Образование:</b> 2005-2009 –Московский Государственный Университет приборостроения и информатики, факультет: информатика, Специальность: прикладная математика
<b>Повышение квалификации:</b> 2009-2012 – Аспирантура при факультете информатики МГУПИ, Специальность: прикладная математика. Кандидат наук 2012-2015 – Докторантура при факультете информатики МГУПИ, Специальность: информационные технологии;
<b>Профессиональные навыки:</b> уверенный пользователь ПК: Photoshop, MS Office, VS 2011, Eclipse, NetBeans IDE, Apache, Nginx, php-fpm, MySQL; высокий уровень знания английского языка.





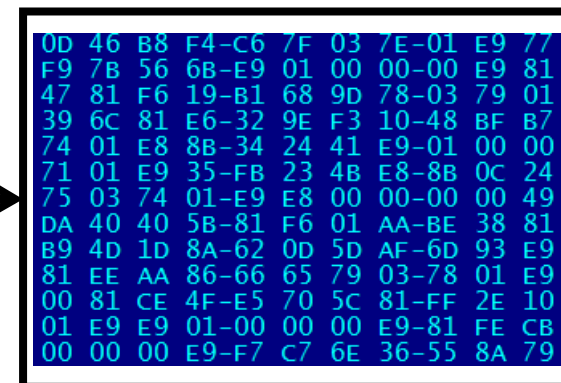




Digitally signed executable



DLL file



File with raw code



## Step 1:

- Hook ntdll.NtQueryDirectoryFile inside explorer.exe

## Step 2:

- Copy previously dropped DLL to following locations:
  - a) %WINDIR%\system32\wbem\loadperf.dll (WinXP)
  - b) %WINDIR%\system32\migwiz\wdscore.dll (Vista+)
- Execute wmiadap.exe(WinXP) or migwiz.exe(Vista+)

```
<requestedPrivileges>  
  <requestedExecutionLevel  
    level="highestAvailable"  
    uiAccess="false"  
  />  
</requestedPrivileges>
```

Win32/Farfli.BEK drops following files:

- %WINDIR%\AppPatch\msimain.mui – raw code
- %WINDIR%\AppPatch\AcProtect.dll

Drops Shim DataBase & registers it:

- %WINDIR%\AppPatch\Custom\%GUID%.sdb



EMET-style sdb (output generated using sdb-explorer by Jon Erickson):

```
44e TAG 7001 - DATABASE
  454 TAG 4023 - OS_PLATFORM
  45a TAG 6001 - NAME: AcProtect_Database
  460 TAG 9007 - DATABASE_ID: {F8C4CC07-6DC4-418F-B72B-304FCDB64052} NON-STANDARD
  476 TAG 7002 - LIBRARY
    47c TAG 7004 - SHIM
      482 TAG 6001 - NAME: AcProtect_Shim
      488 TAG 600a - DLLFILE
  48e TAG 7007 - EXE
    494 TAG 6001 - NAME: twunk_32.exe
    49a TAG 6006 - APP_NAME: AcProtect_Apps
<skipped>
  4d4 TAG 7007 - EXE
    4da TAG 6001 - NAME: explorer.exe
    4e0 TAG 6006 - APP_NAME: AcProtect_Apps
<skipped>
```

Server	IP address	Location
adobeflashupdate.dynu.com	122.10.92.14	Hong Kong
checkpdate.youdontcare.com	122.10.118.129	Hong Kong
csrss.dnsedc.com	122.10.118.131	Hong Kong
dotkang.vicp.net	122.10.118.131	Hong Kong
dwm.dnsedc.com	122.10.118.131	Hong Kong
fsvts.vicp.net		
futuresgolda.com		
gf.arabidc.com	122.10.83.51	Hong Kong
kkts.yeshopea.com	103.225.196.140	Hong Kong
nativeame2.jkub.com	103.225.196.140	Hong Kong
news.bfinancea.net	122.10.118.129	Hong Kong
systemupdate5.dtdns.net		
googlenewsup.net		

Server	IP address	Location
spacecorp.sizn-ru.com		
niisvt.f3322.org	122.10.83.62,103.20.222.170	Hong Kong
note.wikaba.com	122.10.83.62	Hong Kong
systemupdate1.suroot.com	122.10.92.15	Hong Kong
systemupdate1.suroot.com	122.10.92.15	Hong Kong
systemupdate3.suroot.com		
vk.newsupdatea.net	123.254.109.166	Hong Kong
www.dnsqaz.com	122.10.83.62	Hong Kong
www.sizn-ru.com	122.10.83.62, 122.112.2.14	Hong Kong
yahoomessenger.flnet.org	122.10.92.15	Hong Kong
transactiona.com	122.10.92.14	Hong Kong
systemupdate2.etowns.net	122.10.92.14	Hong Kong
adobeupdate1.dtdns.net	122.10.92.15	Hong Kong



Updated Date: **2014-07-28 17:17:48Z**

Creation Date: **2014-07-28 17:17:48Z**

Registrant Name: liu qiuping

Registrant Organization: huajiyoutian

Registrant City: Beijing

Registrant State/Province: BJ

Registrant Postal Code: 100191

Registrant Country: CN

Registrant Email: **yuminga1@126.com**



- We are observing attacks in Russia and CIS countries
- Tip of the iceberg: just one group

### Steps taken:

- Composed IoC
- Contacted CERTs



Special thanks to Cedric Gilbert





cherepanov@eset.sk

