

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

русский киберпреступности



CENTRO CRIPTOLÓGICO NACIONAL





- Comandante Oscar de la Cruz
- Grupo de Delitos Telemáticos
- Unidad Central Operativa - Guardia Civil

Homeland Security News Wire

BIOMETRICS BORDERS BUSINESS CYBERSECURITY DETECTION DISASTERS
INFRASTRUCTURE PUBLIC SAFETY PUBLIC HEALTH SCIENCE SECTOR REPORTS SURVEILLANCE

Cybersecurity

Russian hackers used compromised State Dep. computers to penetrate W.H. systems

U.S. officials said that Russian hackers who penetrated the computer systems of the U.S. State Department in recent months were able to use the access they gained to penetrate parts of the White House computer system. Experts from government agencies looking into the incident say the breach is one of the most sophisticated attacks to have been directed at U.S. government systems. The hackers used computers around the world to mask their penetration, but investigators were able to identify codes and other markers which point to hackers working for the Russian government.

U.S. officials said that Russian hackers who penetrated the computer systems of the U.S. State Department in recent months were able to use the access they gained to penetrate parts of the White House computer system.

The White House has insisted that the breach affected only the White House's unclassified computer system, but experts say that the breach was serious nonetheless. For example, a report posted on the unclassified website of the White House said that the breach was serious nonetheless. For example, a report posted on the unclassified website of the White House said that the breach was serious nonetheless.

CNN reports that back in October, Russian hackers used compromised State Department computers to penetrate White House systems.

Recent stories

Russian hackers used compromised State Dep. computers to penetrate W.H. systems

Computer engineers battle malicious bots

House Democrats write court in support of Obama's immigration executive order

Rwanda: how to deal with a million genocide suspects

Mexican drug war may have increased homicide rates

Predictions of Ebola outbreak overstated by modeling

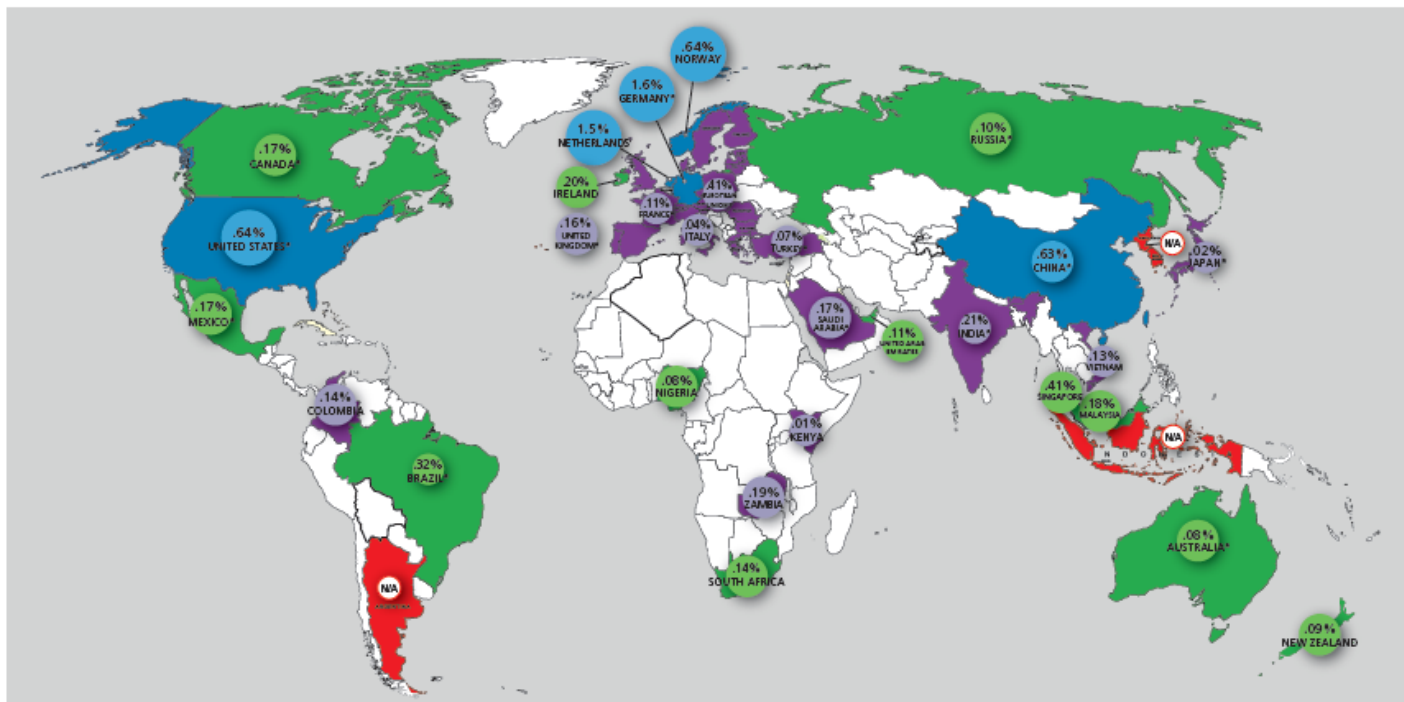
Food safety specialists

ATRIBUCIÓN

Algunas cifras



CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



Confidence Ranking: Countries Current Tracking of Cybercrime within Their Borders.



\$445 BILLION

The annual estimated cost to the global economy from cyber crime



200,000+

Jobs lost in the U.S

150,000+

Estimated in Europe



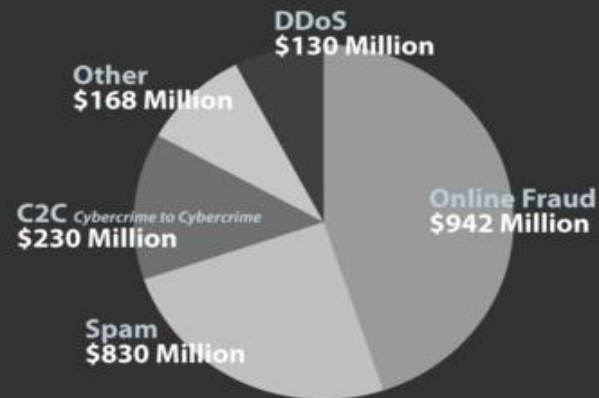
CYBERCRIME

RUSSIAN CYBERCRIME TRENDS

Total Cybercrime Market
IN U.S. DOLLARS



Breakdown of Russian Cybercriminal Activities



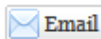




UN POCO DE HISTORIA.....

Hacking Theft of \$10 Million From Citibank Revealed

August 19, 1995 | AMY HARMON | TIMES STAFF WRITER



From a computer terminal in his apartment in St. Petersburg, Russia, a Russian software engineer broke into a Citibank computer system in New York and with several accomplices stole more than \$10 million by wiring it to accounts around the world, according to court documents and the U.S. attorney's office.

Citibank said all but \$400,000 of the stolen funds have been recovered. Six hacking suspects have been arrested, including the engineer, Vladimir Levin, who is being held in Britain and is fighting extradition to the United States.

The incident underscores the vulnerability of financial institutions as they come to increasingly rely on electronic transactions. But computer security experts say what is even more notable about the case is that it became public.

"Can it happen? Yes, it can happen," said a spokesman for the Federal Bureau of Investigation. "But the Citibank case is a warning to all financial institutions."



ert at SRI
erse publicity."

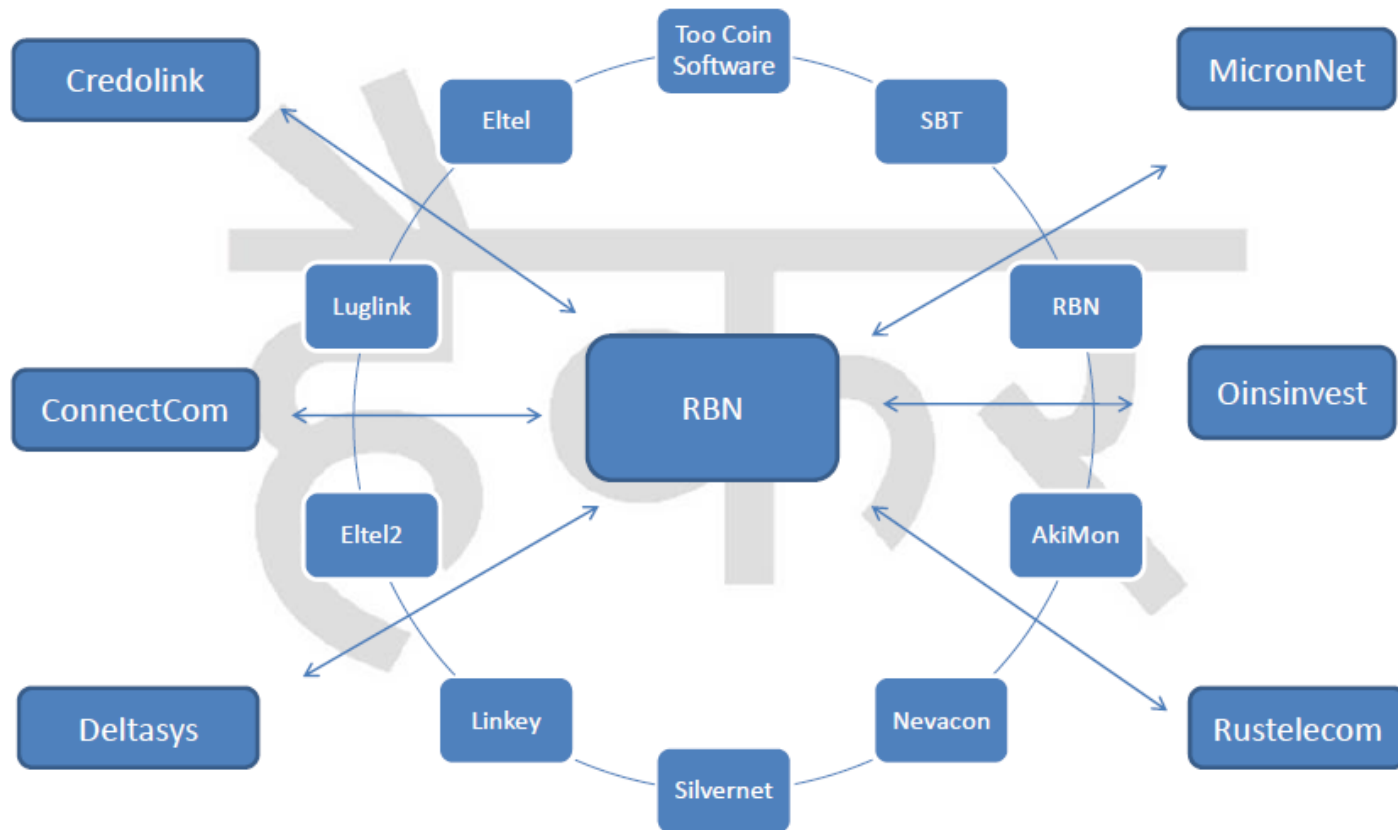
Russian Business Network

- **Russian Business Network – Verisign – “Baddest of the Bad”**
- RBN–2\$ bln (08) & 150\$ mln rev (06-07) ; Criminal ISP
 - Bullet proof hosting
 - Owned by Flyman – nephew of Russian politician
 - Located at #12, Levashovskiv prospect, 197110, St Petersburg, Russia
 - Tracked by Law Enforcement agencies
 - Recruit skilled hackers in Russia for creating malware & exploit 0 days
 - Mysteriously disappeared on 4th Nov 2007 – Believed to be operating under different names
- Google maps image of RBN location



Entramado empresarial

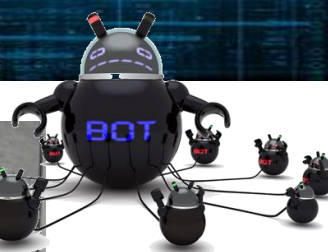
RBN Group Companies



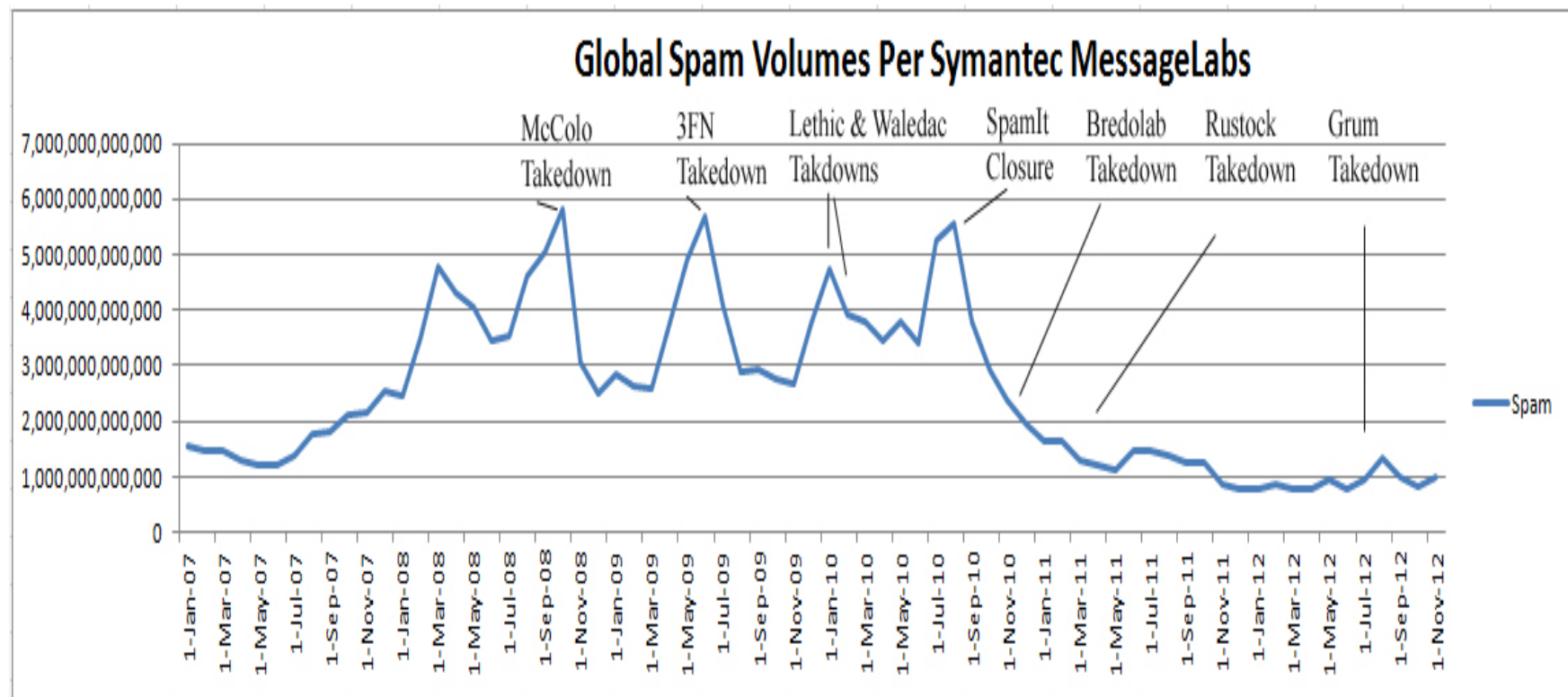




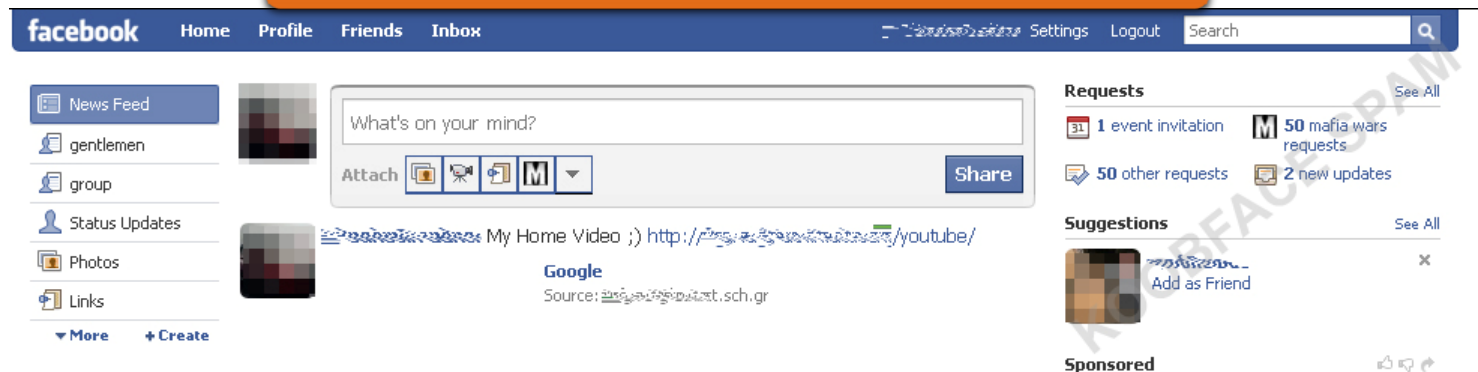
IGOR ARTIMOVICH



PAVEL VRUBLESKY (REDEYE)



KOOFACE



Net- Worm.Win32.Koobface.a, atacaba a MySpace.

Net- Worm.Win32.Koobface.b, ataca a Facebook.

WORM_KOOFACE.DC, ataca a Twitter

Net- Worm.Win32.Koobface .c ataca a www.msn.com

W32/Koobfa-Gen, ataca a Facebook, MySpace, hi5, Bebo, Friendster, myYearbook, Tagged, Netlog y Fubar





BUSINESS MODEL: Cybercrime as a Service

GENERAL		TOPICS	POSTS	LAST POST
	Announcements Info about what's going on...	31	458	by ukakki Tue Nov 03, 2009 2:10 am
	Introductions Introduce yourselfs here.	407	2235	by SNAgger Tue Nov 03, 2009 3:43 am
	Chat / Topic	454	2401	by SNAgger Tue Nov 03, 2009 3:43 am
CARDING MARKET		TOPICS	POSTS	LAST POST
	CC's Sell CC's , Specify Country , Price, Minimum Amount	644	5732	by shubham Tue Nov 03, 2009 4:46 am
	Gift Cards Sell Any Gift Cards in here	233	1248	by spoc Tue Nov 03, 2009 4:24 am
	Cardable Post Sites you've carded here & Chat...	215	1353	by beauty Tue Nov 03, 2009 4:39 am
	Trusted Apply to be a Trusted Member Here...	273	1381	by kate Tue Nov 03, 2009 2:14 am
HACKING		TOPICS	POSTS	LAST POST
	Bot Bin/Sources + Bots	107	885	by ukakki Tue Nov 03, 2009 1:35 am
	Stealers / Keyloggers / Rats	65	381	by pikachu Tue Nov 03, 2009 12:12 am
	Accounts Sell Cpanel/WHM's etc here...	432	1239	by Tue Nov 03, 2009 2:55 am
	Crypters/Downloaders Sell Bankers/Counter etc here... No new posts	48	326	by Sp00k13 Mon Nov 02, 2009 6:57 pm
	Servers and Hosting Sell Servers/Routers etc here...	93	364	by kate Tue Nov 03, 2009 2:16 am
	Other Sell Other stuff here, which doesn't fit in other categories, eg. Databases	251	1063	by Pkachu Tue Nov 03, 2009 2:54 am
	Exploits Sell 0day Exploits here...	28	240	by kate Mon Nov 02, 2009 6:55 pm
PHISHING MARKET		TOPICS	POSTS	LAST POST
	Bank Logins Sell Any Bank Login here...	432	2296	by SNAgger Tue Nov 03, 2009 12:37 am
	Phishing Kits Post Free Phishing Kits + Sell em...	35	183	by SNAgger Wed Oct 28, 2009 12:20 pm
	Emails / Spamming Sell Fresh Email Lists etc here...	159	622	by ukakki Tue Nov 03, 2009 2:48 am

FOROS CARDING

Logout

Messages

Your Balance:
 Shopping Cart: 0 Item(s) - \$0.00

SEARCH CARDS

BIN (+\$0.50)	COUNTRY (+\$0.00)	STATE (+\$0.00)	CITY (+\$0.00)	ZIP (+\$0.20)
	Australia (554 cards)			

☐ Have SSN
 ☐ Have DoB

U.S.-Based Credit Card Prices by Brand

Site	Visa/MasterCard	AMEX	Discover
Site 1	US\$1.50/card	US\$2.00/card	US\$3.00/card
Site 2	US\$1.00/card	US\$1.20/card	US\$1.50/card
Site 3	US\$2.00/card	US\$2.50/card	US\$2.50/card
Site 4	US\$2.00/card	US\$3.00/card	US\$3.00/card

	408531***** (No Category)	Derek	Australia	Victoria	Melbourne	3182	NO	NO	\$4.50	☐
	434968***** (No Category)	clare	Australia	Western Australia	Mundaring Perth	6073	NO	NO	\$4.50	☐
	493414***** (No Category)	Martine	Australia	NSW	Concord	2137	NO	NO	\$4.50	☐
	494052***** (No Category)	Antony	Australia	Victoria	Melbourne	3078	NO	NO	\$4.50	☐
	494053***** (No Category)	Kathy	Australia	QLD	Brisbane	4152	NO	NO	\$4.50	☐
	423953***** (No Category)	Melinda	Australia	NSW	Seaforth	2092	NO	NO	\$4.50	☐
	450949***** (No Category)	Michelle	Australia	NSW	Sydney	2029	NO	NO	\$4.50	☐

Add Selected Cards to Shopping Cart

Shop website	Mirrors	Type of shop	Total cards	Card upload period	Shop turnover
https://rescator.cm/	Rescator.so Rescator.cc Octavian.so Octavian.cm	Card dumps	79 357	07.2014-06.2015	\$532 644
https://swipebz.org/		Card dumps	28 715	11.2014-06.2015	\$192 735
http://zeon.io		Card dumps	18 761	02.2015-06.2015	\$125 924
www.validcc.su		Card dumps	28 916	09.2014-06.2015	\$194 084
http://tormarket.cc/	ccguru.su cardmarket.cc dvshop.su getcvvs.ru	Card Text data	207 311	07.2014-06.2015	\$139 147
https://cvv.me		Card Text data	206 9740	07.2014-06.2015	\$1 389 209
http://centralshop.cn/	mr-anderson.cn qhd6aon2fyjjan4e. onion	Card Text data	225 086	11.2014-06.2015	\$151 078

Net turnover:

\$2 724 822



VLADIMIR DRINKMAN

Detenido en Holanda en 2012

Extraditado a USA en Enero 2015

US Accused of 'Kidnapping' Russian Hacker Roman Valerevich Seleznev Following Arrest



By *David Gilbert*

July 8, 2014 12:31 BST





RANSOMWARE

CoinVault

13



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95 50 03

Next >>



CAMPAÑA DISTRIBUCIÓN



Su paquete ha llegado **06 de abril**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.



CD 000312844452

[Descargar información sobre su envío](#)

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para el día manteniendo en la cantidad de 7,55 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Condiciones y Términos del Servicio de localización de envíos

Por medio del presente aviso, la Sociedad Estatal Correos y Telégrafos S.A. (en adelante, Correos) informa de su política de protección de los datos de carácter personal a fin de que los usuarios puedan elegir libre y voluntariamente si desean comunicar a Correos los datos personales que se le soliciten con ocasión de la suscripción de servicios ofrecidos a través del sitio web www.correos.es. Se advierte a los usuarios que alguno de los servicios ofrecidos a través del sitio web, pueden incluir condiciones particulares en materia de protección de datos de carácter personal. El acceso a dichos servicios, implicará la aceptación de las condiciones particulares establecidas para los mismos. El usuario garantiza que los datos personales que facilite a Correos son veraces y que comunicará cualquier modificación que afecte a los mismos. En consecuencia, Correos se exonera de cualquier responsabilidad derivada del incumplimiento por el usuario de esta garantía. Los datos que faciliten los usuarios serán incorporados a un fichero automatizado de datos de carácter personal cuya titularidad corresponde a Correos, con la finalidad de gestionar los servicios contratados. En los formularios se indicará el carácter obligatorio o facultativo de los campos a cumplimentar.

[Haga clic aquí para](#) darse de baja.

THE **FBI** FEDERAL BUREAU OF INVESTIGATION



REPORT THREATS • A-Z INDEX • SITE MAP

Search Site

Q SEARCH

CONTACT US

ABOUT US

MOST WANTED

NEWS

STATS & SERVICES

SCAMS & SAFETY

JOBS

FUN & GAMES

Wanted by the FBI

Seleccionar idioma ▾

✉ Get FBI Updates

Home • Most Wanted • Cyber's Most Wanted

Cyber's Most Wanted

Select the images of suspects to display more information.



EVGENIY
MIKHAILOVICH
BOGACHEV



NICOLAE
POPESCU



ALEXSEY
BELAN



ARTEM
SEMEV



VIET QUOC
NGUYEN



SUN KAILIANG



HUANG ZHENYU



WEN XINYU



WANG DONG



GU CHUNHUI

Show All



EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy, Computer... more —

REWARD: The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to \$3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

Evgeniy Mikhailovich Bogachev, using the online monikers "lucky12345" and "slavik", is wanted for his alleged involvement in a wide-ranging racketeering enterprise and scheme that installed, without authorization, malicious software known as "Zeus" on victims' computers. The software was used to capture bank account numbers, passwords, personal identification numbers, and other information necessary to log into online banking accounts. While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised web sites. Victims who visited these web sites were infected with the malware, which Bogachev and others utilized to steal money from the victims' bank accounts. This online account takeover fraud has been investigated by the FBI since the summer of

SUMMARY

ALIASES

DESCRIPTION

MORE

PHOTOS

GET POSTER

НА РУССКОМ

на

українській

мові

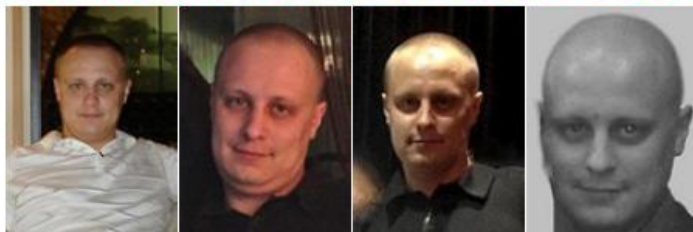
SUBMIT A TIP

WANTED

BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV



Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth October 28, 1983

Used:

Height: Approximately 5'9"

Weight: Approximately 180 pounds

NCIC: W890989955

Occupation: Bogachev works in the Information Technology field.

Hair: Brown (usually shaves his head)

Eyes: Brown

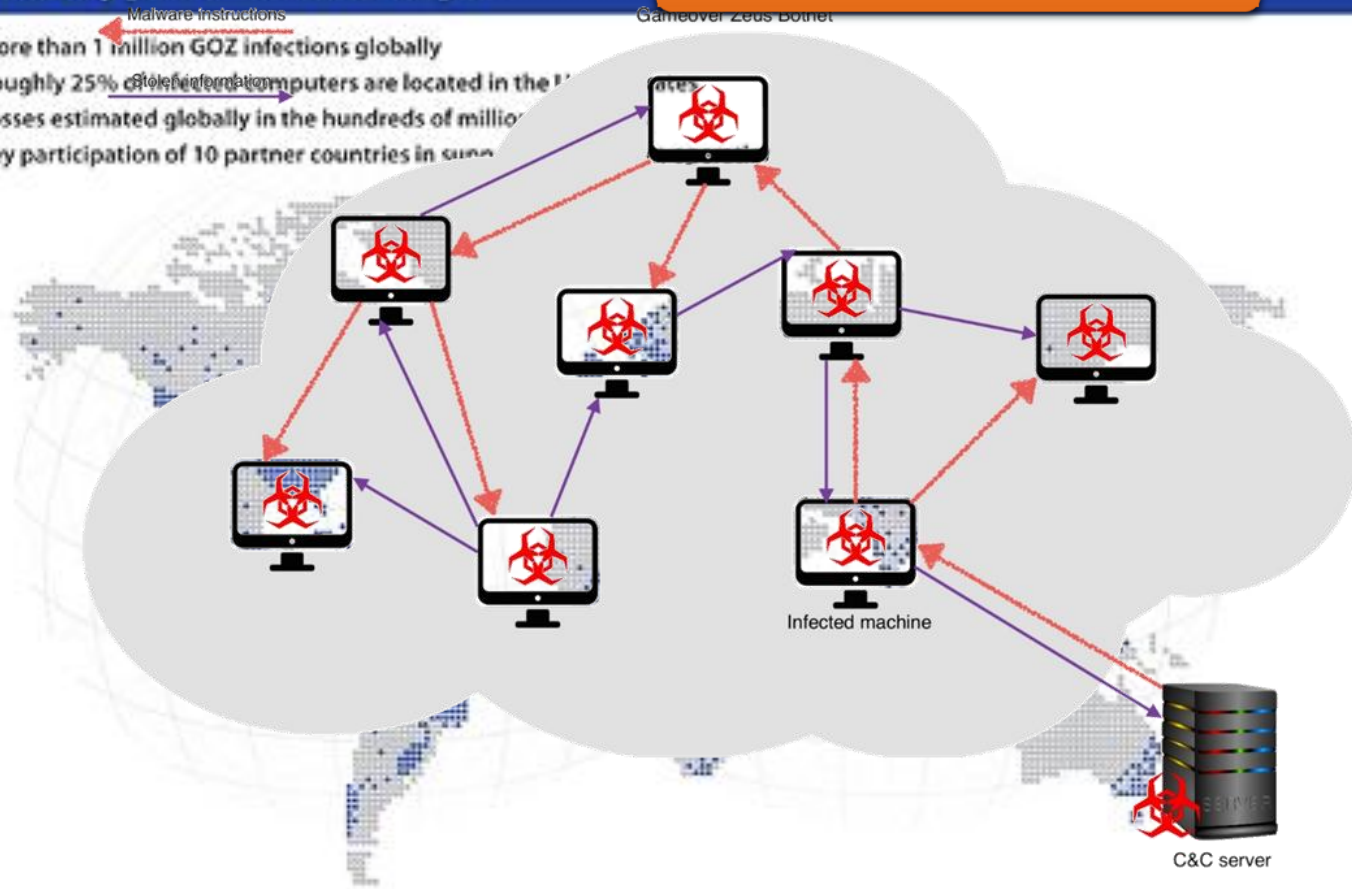
Sex: Male

Race: White

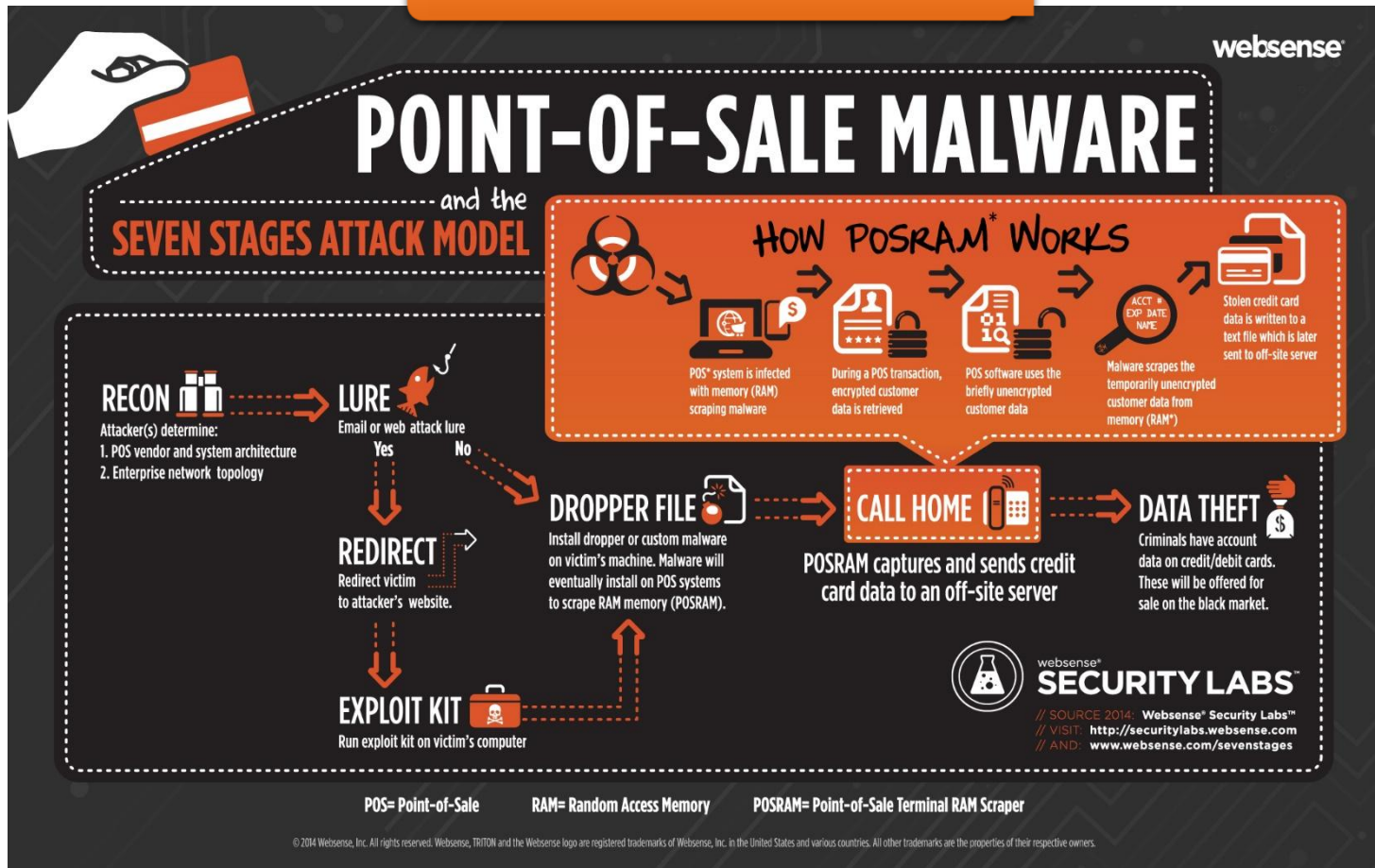
GOZ/CryptoLocker Scope

- More than 1 million GOZ infections globally
- Roughly 25% of infected computers are located in the U.S.
- Losses estimated globally in the hundreds of millions
- Key participation of 10 partner countries in GOZ

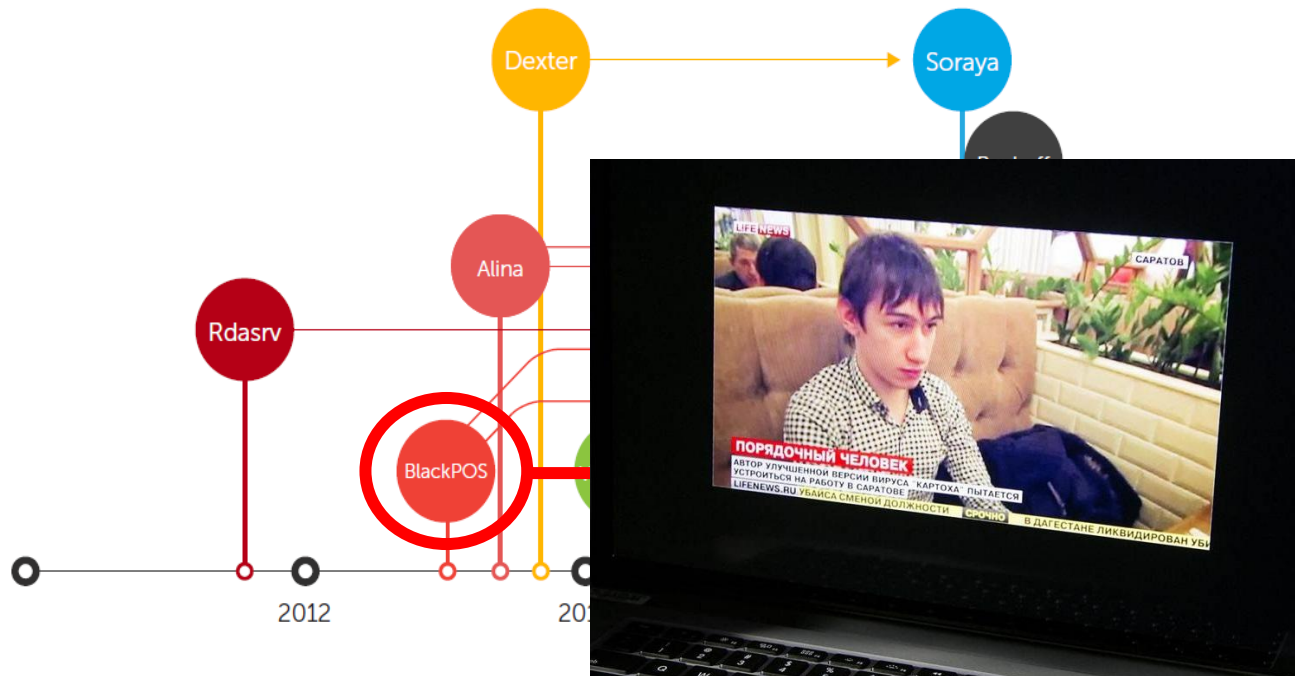
GAME OVER ZEUS (GOZ)



POS MALWARE

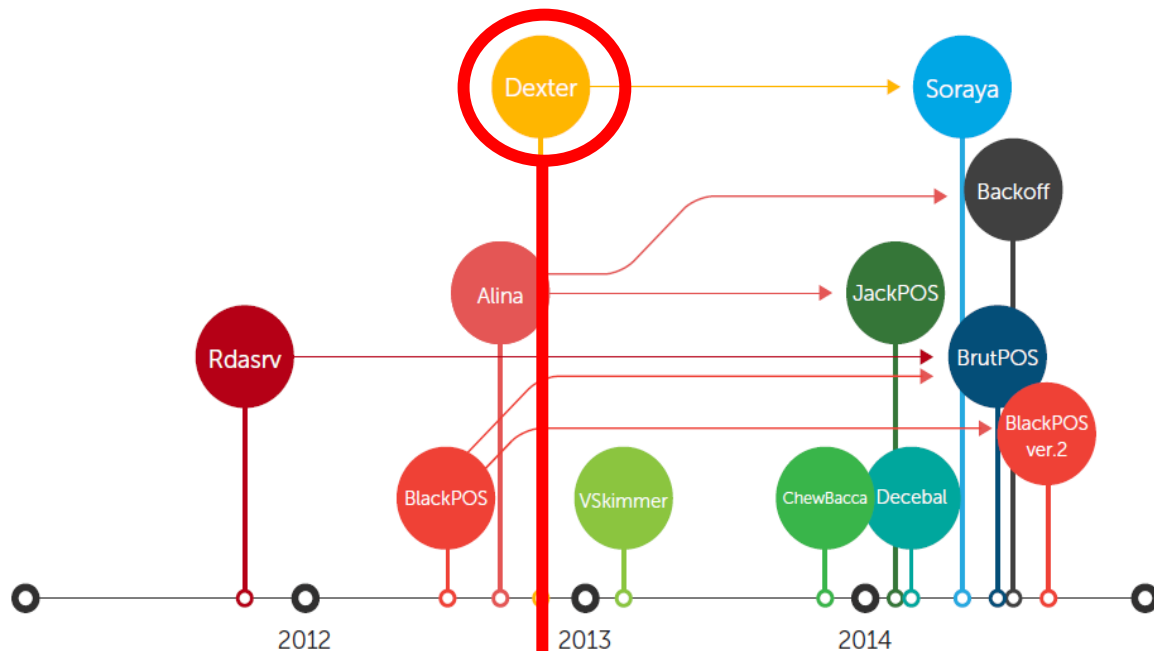


EVOLUCIÓN POS MALWARE



SERGEY TARASPOV (17a)

EVOLUCIÓN POS MALWARE



EVOLUCION CAMPAÑAS CONTRA BANCOS



ANUNAK

INFORME



FOX IT

FOR A MORE SECURE SOCIETY

GROUP IB

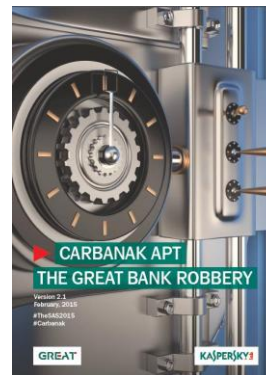
Ataques al sector bancario

1er suceso KIEV ENE'13

2º Informe Kaspersky

Carberp + Anunak : Karbanak

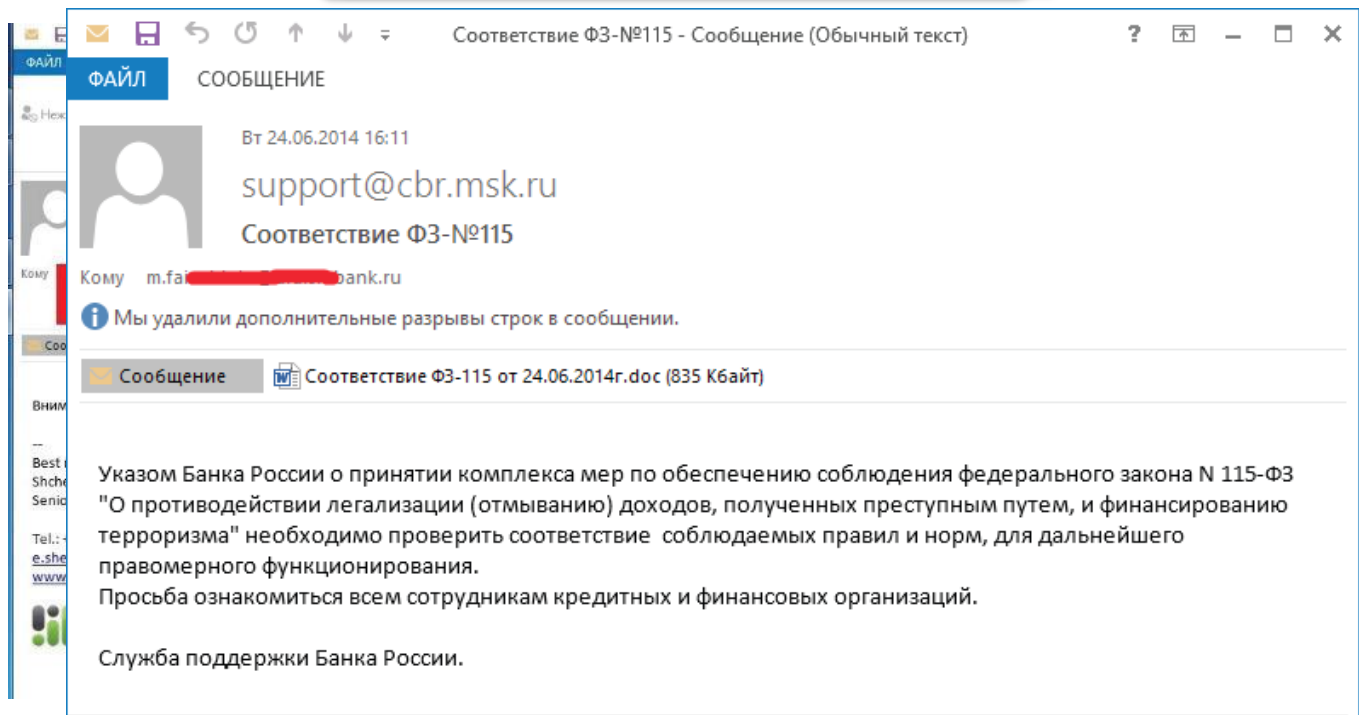
PROCESO



1

Infección de un empleado

CORREOS CON MALWARE



CVE-2012-0158

CVE-2012-2539

CVE-2014-1761

www.ccn-cert.cni.es

ANUNAK

2

Obtener password user con privilegios

3

Conseguir acceso a correo y servidores

4

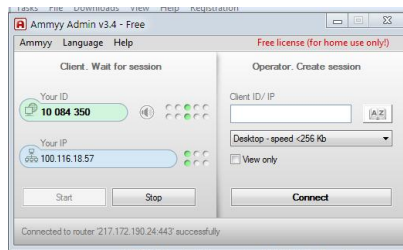
Escalada privilegios, admin



ANUNAK

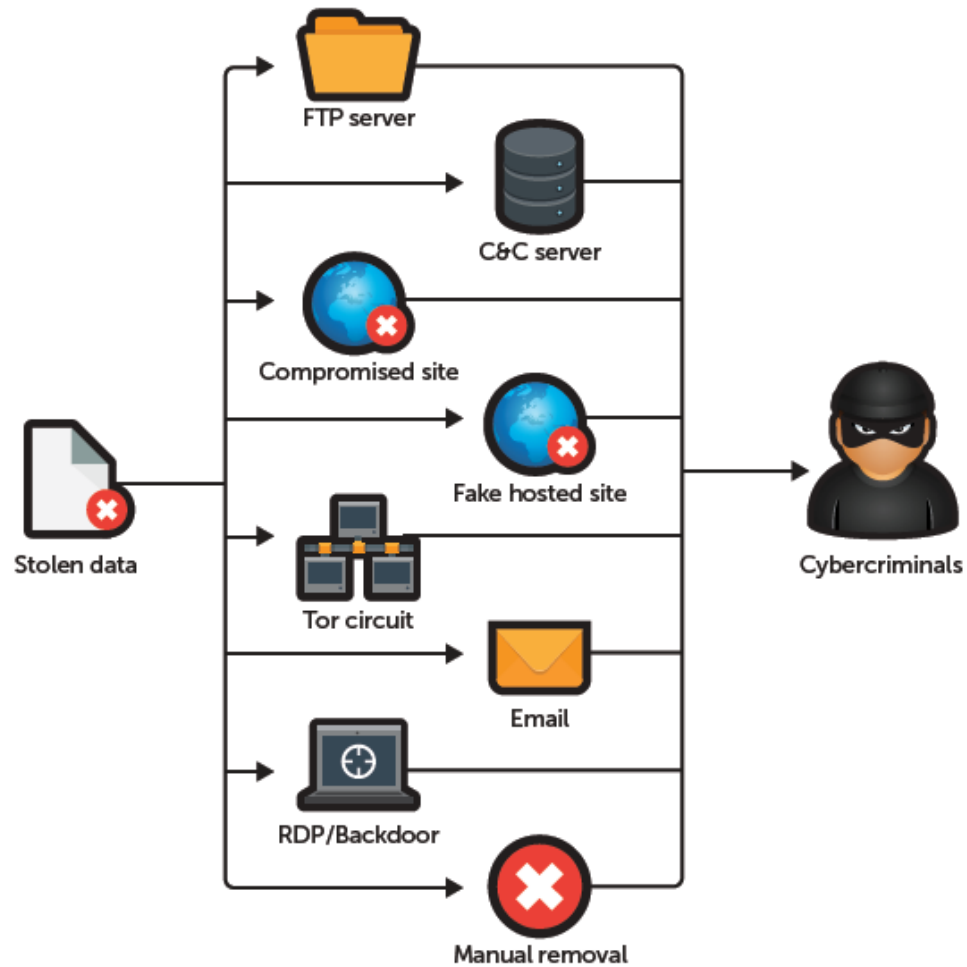
5

Instalación software RAT



6

Configuración accesos remotos y firewall



Rusia ofrece 110 mil dólares al que logre hackear la red anónima Tor

El gobierno ruso lanzó un concurso público para "desanonimizar" la red Tor -que protege la privacidad de sus usuarios en Internet- y así identificar a quiénes la usan, con el argumento de proteger la seguridad nacional.

[Recomendar](#)

170

[Tweet](#)

40

[g+](#)

11



ACCESIBLE



EL ORIGEN DE TOR??



ANUNAK

\$ 1 000 000 000



EXPLOTACIÓN

3. Suplantación del empleado

Cómo robaron el dinero

Banca online

Dinero transferido a las cuentas de los ciberpiratas

Sistemas de pago electrónico

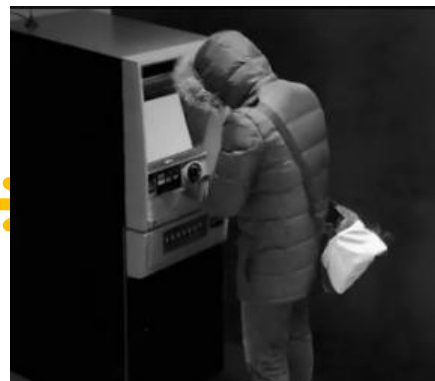
Dinero transferido a bancos en EE.UU. y China

Aumento de saldos en cuentas

Fondos adicionales extraídos mediante transacciones fraudulentas

Control de cajeros automáticos

Instrucciones para entregar efectivo en un momento predeterminado



ANUNAK

ANUNAK

Clave cifrado RC4

754037e7be8f61cbb1b85ab46c7da77d

Search Form

NOTE: *This page is limited to 20 queries per one(1) hour time period.*

md5 hash 754037e7be8f61cbb1b85ab46c7da77d = go fuck yourself

Enter a md5 or sha1 hash:

754037e7be8f61cbb1b85ab46c7da77d

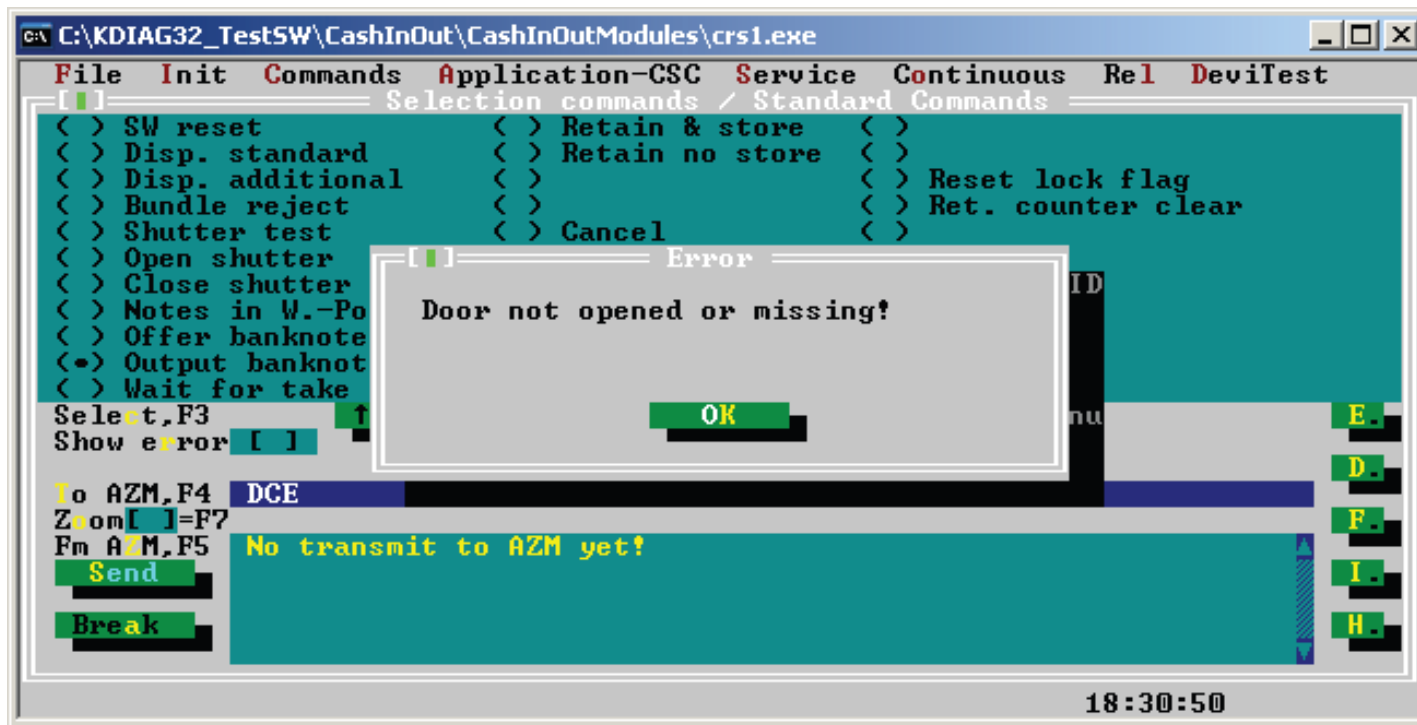
Submit

Current "Hit Rate": 100 %

Size of database: 20,621,101 words

CONTROL DE CAJEROS

Acceso VPN desde equipos infectados Software ATMs Wincor-Nixdorf

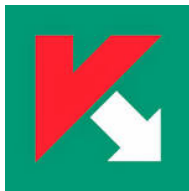




ATM MALWARE



TYUPKIN'



CAJEROS NCR
Win32

BootCD

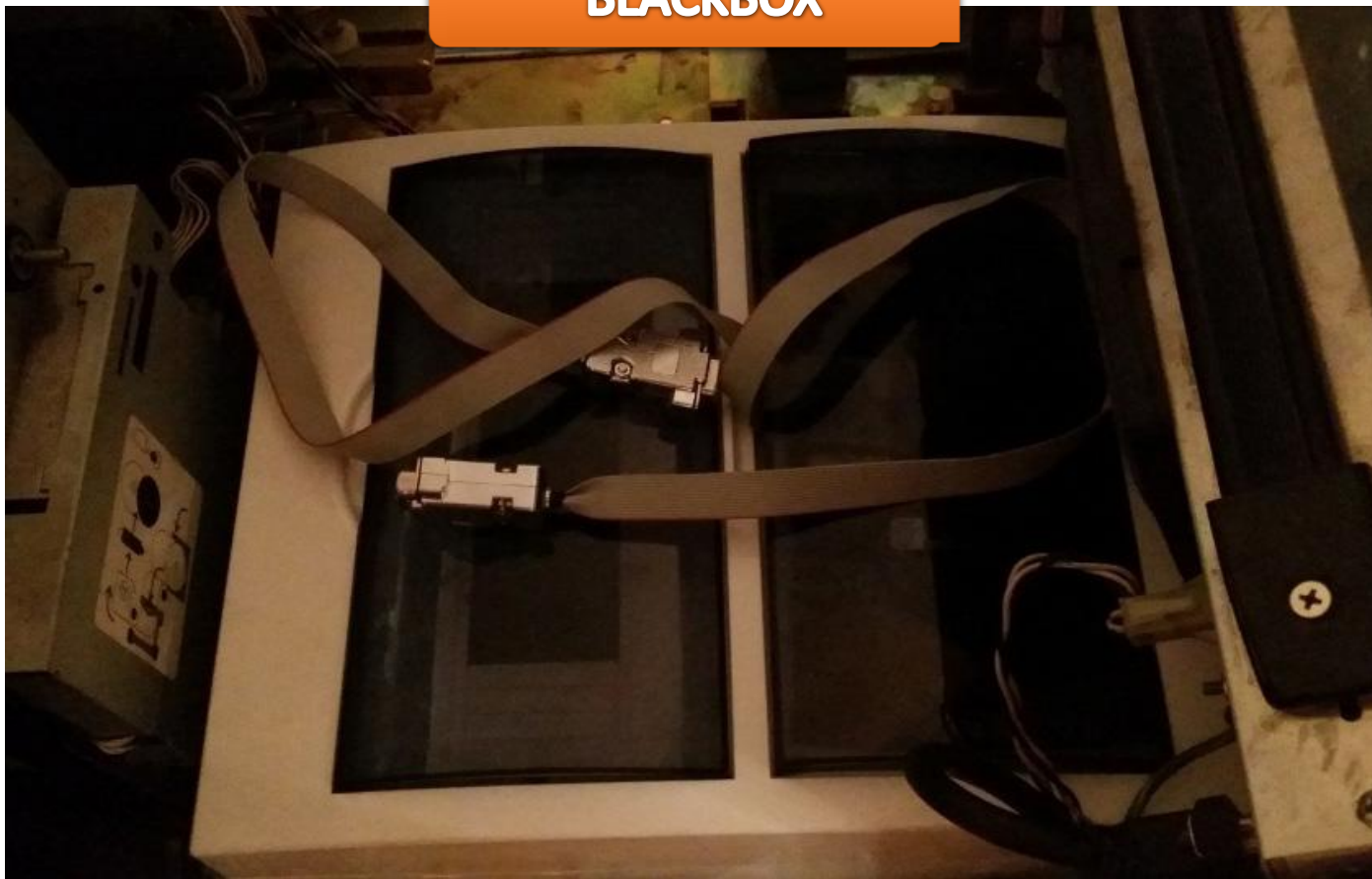
PINCode
1am – 5am



TYUPKIN'

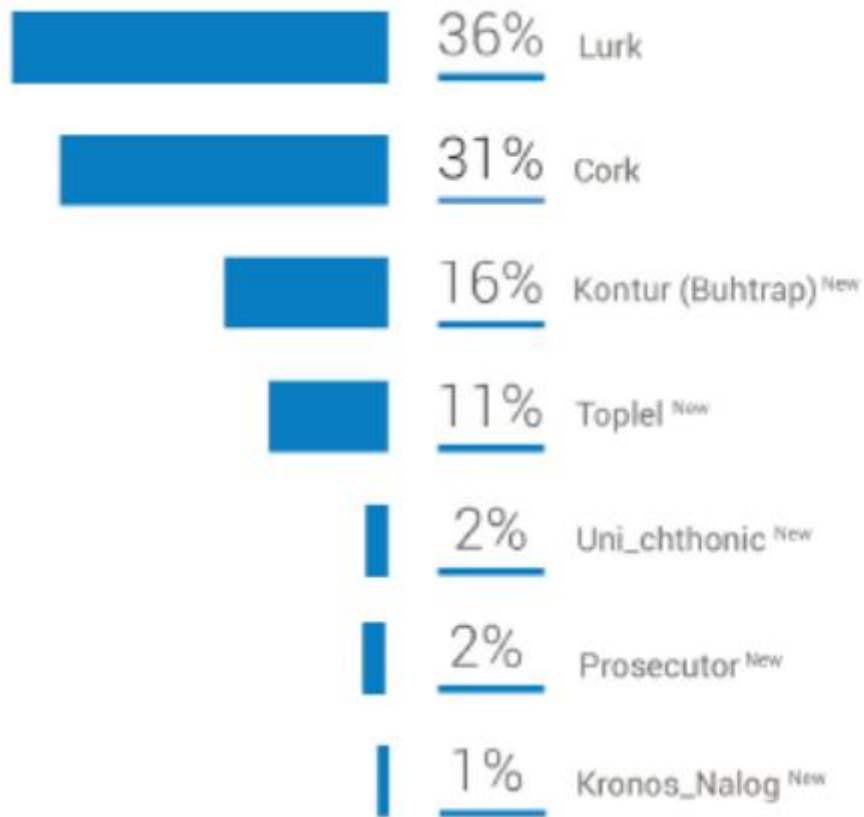


BLACKBOX



Malware	Threat Level	Primary Function	Primary Infection Vector	Aliases/Variants	Trend
Cryptolocker	HIGH	Ransomware	Email attachment	-	▲
DarkComet	HIGH	RAT	Exploit kit	Fynloski, Fynlos, Krademok, DarkKomet	▲
Dridex	HIGH	Data Stealer	Email attachment (Word macros)	Bugat, Feodo, Cridex	▲
Zeus	HIGH	Data Stealer	Exploit kit	Zbot, Gameover (GOZ)	↔
Blackshades	HIGH	RAT	Exploit kit	-	▼
Citadel	HIGH	Data Stealer	Exploit kit	-	▼
SpyEye	HIGH	Data Stealer	Dropper	-	▼
CTB-Locker	MEDIUM	Ransomware	Email attachment (.zip)	Critroni	▲
Dyre	MEDIUM	Data Stealer	Dropper (UPATRE)	Dyreza	▲
Tinba	MEDIUM	Data Stealer	Exploit kit	Tinybanker, Zusy	▲
Carberp	MEDIUM	Data Stealer	Exploit kit	-	↔
Shylock	MEDIUM	Data Stealer	Exploit kit	Caphaw	↔
Ice IX	MEDIUM	Data Stealer	Exploit kit	-	▼
Torpig	MEDIUM	Data Stealer	Exploit kit	Sinowal, Anserin	▼

GRUPOS MÁS ACTIVOS



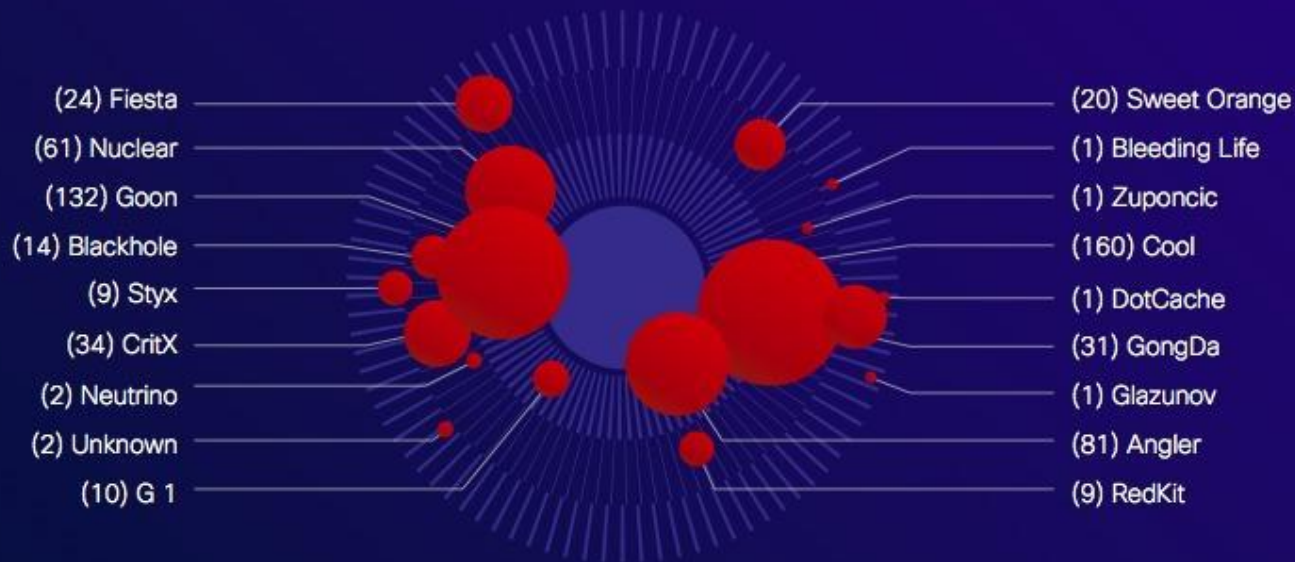
Trojan	Total groups
Dyre (Dyreza)	1
Dridex (Bugat, Feodo, Cridex)	>3
Qadars	1
Emotet	1
Vawtrak (Neverquest, Papras)	4
ISFB (Ursnif)	3
Kronos	2
MMBB (Money Maker Bank Bot)	2
Tinba (Zusy)	>8
Zeus 2.0.8.9	>11
Citadel	>17
KINS (ZeusVM)	>18



EXPLOIT KITS

Exploit Kits Observed Since January 2014

SOURCE: Cisco Threat Intelligence Platform



(# of attacks) Exploit Kit Name

Black hole ¹⁵ СТАТИСТИКА ПОТОКИ ФАЙЛЫ БЕЗОПАСНОСТЬ НАСТРОЙКИ Выйти

Начало: Конец: Применить Автообновление: 10 сек.

СТАТИСТИКА

ЗА ВСЁ ПЕРИОД

1431571 ХИТЫ **705823** ХОСТЫ **41702** ЗАГРУЗКИ **7.5%** ПРОБИВ

ЗА СЕГОДНЯ

338149 ХИТЫ **187835** ХОСТЫ **11531** ЗАГРУЗКИ **8.35%** ПРОБИВ

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Windows 7	712116	362252	16234	5.37
Windows XP	393107	197132	16103	9.92
Windows Vista	206019	108832	9365	10.25
Другое	120284	42960	0	0.00

ПОТОКИ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
	661685	263494	16054	9.65
	174864	172008	10032	6.04
	391958	115356	3783	5.73
	64030	60184	4732	8.57
	62345	59729	3455	6.55
	56669	52096	3502	7.42
	2367	2274	91	6.77
	936	920	50	6.33
	16595	127	0	0.00
	50	50	0	0.00
	3	2	1	100.00

ЭКСПЛОИТЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
FLASH	448	1.07		
HCP	508	1.22		
Java Array	26687	63.99		
MDAC	434	1.04		
PDF ALL	2781	6.67		
PDF LIBTFF	10844	26.00		

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
MSIE	600584	336431	30776	9.53
Firefox	496513	255361	10926	4.69
Другое	334419	120374	0	0.00

СТРАНЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Germany	464805	228627	12842	6.70
Italy	166974	97303	6077	7.75
France	186984	95339	4601	6.02
Spain	194397	90555	6700	9.89
United Kingdom	54448	49645	2834	5.95
Canada	91891	42336	2556	8.17
Portugal	64153	27640	2067	9.95
Belgium	58437	25295	1717	8.95
Greece	31604	14730	1055	10.30
Austria	28234	10478	844	10.82
Netherlands	27949	7318	0	0.00
Finland	18233	6583	375	8.76
Other country	9152	4537	0	0.00
Australia	7745	2263	0	0.00
United States	20055	1972	2	100.00
Другое	6485	1188	32	7.34



PAUNCH

> 1000 Clientes

> 50.000\$ benef./mes



Nuclear Pack v2.0

Настройки

Селлеры

Url for traffic

API

Очистить

Выход  

Load1

Load2

Load3

Load4

Load5

Load6

Глобальная статистика



Statistic for seller:

Загрузка файла

Обзор...

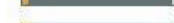
Загрузить

Размер Файла: 40 Kb

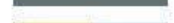
MD5: 80c8eac98ebcbc5019c19e3da0b02cd6

Подробная статистика

СТРАНЫ(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
 US	15353	11571	1194	 10.32%

БРАУЗЕРЫ(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
 MSIE 9.0	6347	4978	603	 12.11%
 MSIE 8.0	2734	2126	286	 13.45%
 Firefox 11.0	2697	2275	106	 4.66%
 MSIE 7.0	1766	940	69	 7.34%
 Opera 9.80	476	288	42	 14.58%

ОС(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
 Windows 7	8959	7062	717	 10.15%
 Windows XP	3199	2424	216	 8.91%
 Windows Vista	2863	2055	265	 12.9%
 Windows 2003	316	170	1	 0.59%
 Windows 2000	16	12	0	 0%

РЕФЕРАЛЫ(TOP 10)	ВСЕГО	УНИК.	ЗАГРУЗКИ	
	7758	6495	725	 10.15%
	7578	6552	613	 9.91%
	4	4	0	 0%
	3	2	1	 33.33%
	2	2	0	 0%

HAMMERTOSS



DRIDEX Infection Chain



DRIDEX arrives onto systems as malware downloaded by a malicious spam attachment.

The downloading is done through the malicious macro embedded in the .DOC attachment (detected as TROJ_WMSHELL.A).

Once DRIDEX is downloaded and installed, it injects malicious codes onto the system's browser, to steal online banking login credentials.

DRIDEX also performs form grabbing, screenshots and clickshots in order to steal more personal information from the affected system.

Man in the Browser



Website seen
by Customer

Anybank - Windows Internet Explorer

www.anybank.com

File Edit View Favorites Tools Help

Anybank

Online banking

Payment Details

To pay someone please enter the following details

Payee name:

Payee account no.:

Payee sort code:

Amount:

My Computer 100%



Website seen
by Bank



Anybank - Windows Internet Explorer

www.anybank.com

File Edit View Favorites Tools Help

Anybank

Online banking

Payment Details

To pay someone please enter the following details

Payee name:

Payee account no.:

Payee sort code:

Amount:

**! Customer makes the transfer
but malware changes
destination and amount**

LEGISLACIÓN

Chapter 28 Criminal Code of Russian Federation.

Crimes related to computer information



Art. 272. Illegal access to computer information

Art. 273. Creating, use and dissemination of malware

Art. 274. Computers, computer systems and nets exploitation rules violation



PHISEYE



Статистика
Боты
Команды
Отчеты
Опции

Сообщения (0)
Коллектор (0)

Общая статистика

Количество ботов всего, онлайн.

Ботнет	Всего
Всего ботов	19895
Ботов в сети	3901
Активных за 24ч	8354
% Онлайн	20%
% Активных	42%

Страны

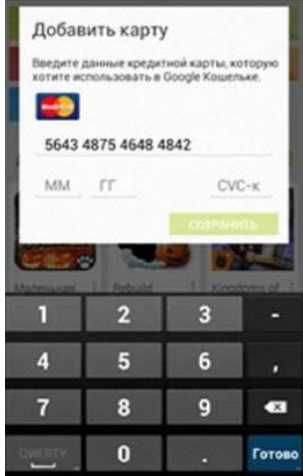
Статистика стран ботов.

Страна	Количество
RU	9781
XX	5042
UA	4378
UZ	96
FR	69
TR	61
GE	50

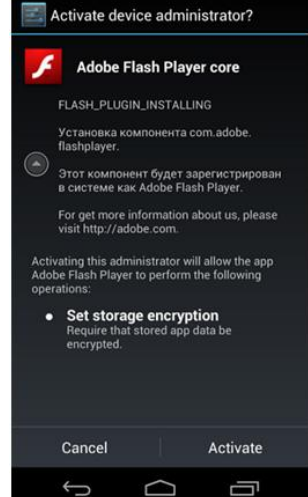
Операторы

Статистика операторов ботов.

Оператор	Количество
Android	6203
Beeline	1754
MTS	1671
MegaFon	1348
TELE2	1027
MTS_UKR	877
lifel	826







COOPERACIÓN POLICIAL

Mº INTERIOR

DEPARTAMENTO K



FSB



Centro Nacional de Coordinación de Incidentes
informáticos



International cooperation and Interaction

Ministry of Interior of Russian Federation



Department «K»



Interpol



NCP G8 24/7



Liaison officers



International investigation order



General office of Public Prosecutor





Grupo de Delitos
Telemáticos de la Guardia
Civil

Siguiendo

1.527 seguidores



Más info

Fotos oficiales



Escribe un comentario...



Grupo de Delitos Telemáticos de la Guardia Civil
#GDTweetDelDia La Colaboración Ciudadana es fundamental. ¡NO COMPARTAS Vídeos Sexuales!, repórtalo



Grupo de Delitos Telemáticos de la Guardia Civil
En muchas ocasiones os hemos agradecido vuestra ayuda, es fundamental para nosotros. Pero la colaboración tiene líneas que no debéis traspasar con frecuencia, es la de informar sobre cor

Escribe un comentario...



Grupo de Delitos Telemáticos

A 54.910 personas les gusta esta página · 2.988 personas están hablando sobre esto

Organización Gubernamental
Con tu ayuda, haremos de Internet un lugar más seguro. Informarnos en nuestra web: www.gdt.guardiacivil.es

Información

Fotos

Videos

Lo más destacado

Estado Foto / video Oferta, Evento +

¿En qué estás pensando?



Grupo de Delitos Telemáticos compartió un enlace.
Martes 19

#GDTweetDelDia La Colaboración Ciudadana es fundamental, pero ojo con los límites. ¡NO COMPARTAS Vídeos Sexuales!, repórtalo en nuestra web

GDT - Grupo de Delitos Telemáticos
www.gdt.guardiacivil.es

Me gusta



Organización Gubernamental



Informática64 SL
Computadoras/Tecnología



Panda Security

IX JORNADAS STIC CCN-CERT

www.gdt.guardiacivil.es



Buscar ¿Tienes cuenta? Iniciar sesión

Tweets
Siguiendo
Seguidores
Favoritos
Listas

Sigue a GDT Guardia Civil

Nombre completo

Correo electrónico

Contraseña

Regístrate



Ver todas las fotos y videos

Tendencias Globales · Cambiar

#voteshopPayDust

#voteshopConCocaColaFACIL

#voteshopESCALA

#voteshopvoteshopThat

#voteshopvoteshopThat

Paraná Wants Where We Are Tour 2014

Chris Bryant

Andrés Nasser Capalio de Enríquez

Philip Hammond

M&G



376 TWEETS 43 SIGUIENDO 45.719 SEGUIDORES

Siguir

Tweets todos Sin menciones

GDT Guardia Civil @GDTGuardiaCivil
#GDTweetDelDia La Colaboración Ciudadana es fundamental, pero ojo con los límites. ¡NO COMPARTAS Vídeos Sexuales!, repórtalo en nuestra web

GDT Guardia Civil @GDTGuardiaCivil
#GDTweetDelDia ¡ATENCIÓN! Nuevo #PHISHING suplantando MOVISTAR. Mail alertando de un error en la facturación dirige a web que pide tus datos

GDT Guardia Civil @GDTGuardiaCivil
#GDTweetDelDia ¿Has visto tus datos en Internet (teléfono, dirección, mail, fotos)? #DERECHOALOLVIDO, pide que se retiren, o ¡DENÚNCIALO!

GDT Guardia Civil @GDTGuardiaCivil
#GDTweetDelDia ¿Los contactos han recibido un mensaje tuyo pidiendo ayuda? ¡TE HAN ROBADO LA CUENTA! Cambia la contraseña y ¡DENÚNCIALO!

Lleida.net @lleidaport
05/10 w'll speak @FOSE about our registered ecommunications & @GDTGuardiaCivil CybercrimeUnit bit.ly/10NyJb Join us



@GDTGuardiaCivil

www.ccn-cert.cni.es

GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL