

KNOWLEDGE
INSIDE



www.knowledgeinside.pt

MAKE IT MORE VALUABLE

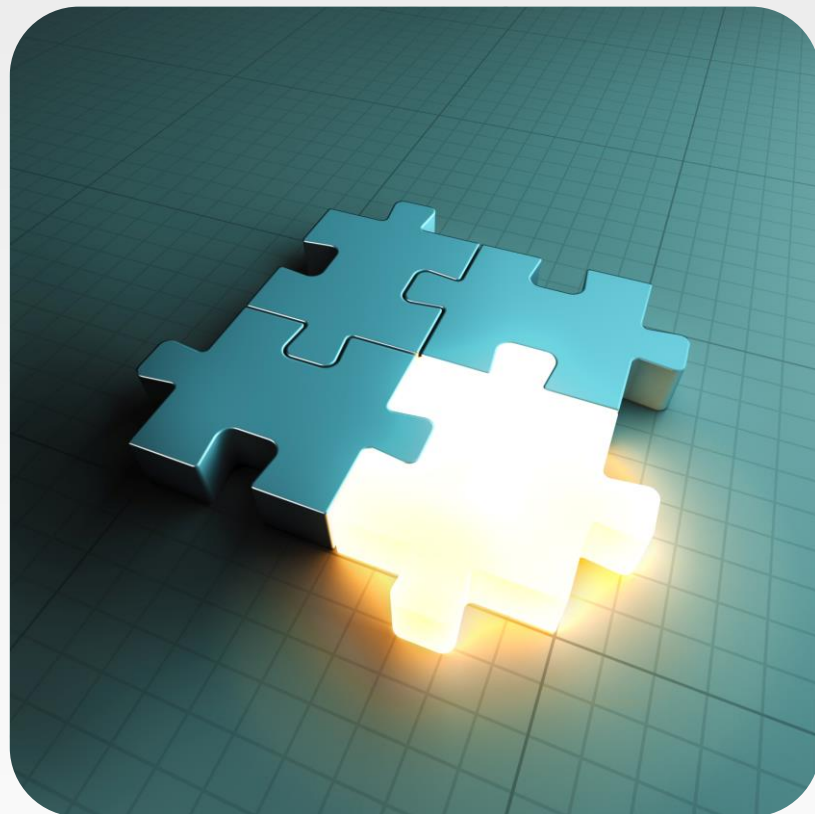
SOBRE A KNOWLEDGE INSIDE

A **Knowledge Inside** é uma empresa fornecedora de serviços e soluções tecnológicas especializada em infraestrutura e soluções Cloud da Microsoft.

A empresa opera também enquanto fornecedor de serviços Cloud e MSP, onde se destacam as soluções **NIODO** e o **KI Servicedesk**, onde serviços e infraestrutura de TI são entregues chave-na-mão às PME.

A empresa possui uma **equipa muito experiente** e altamente especializada, com **várias certificações** Microsoft e Citrix, nomeadamente Microsoft Certified Technology Specialist, Microsoft Certified IT Professional, Microsoft Certified Systems Administrator, Microsoft Certified Systems Engineer e Citrix CSA.

De forma a melhor servir o mercado, **conta com várias parcerias estratégicas**, das quais se destacam empresas como a Microsoft, Citrix, Symantec, GFI, Veeam, HP, DELL, EMC





RANSOMWARE – OS MEUS FICHEIROS FORAM RAPTADOS E AGORA?



O QUE É?

Ransomware é uma forma de software malicioso com capacidade de “raptar” os dados do computador infetado. Funciona impedindo o acesso aos ficheiros e a certas funções críticas do sistema ou em alguns casos a todo o computador. Para recuperar o acesso aos ficheiros ou ao sistema é exigido à vítima que **pague um resgate**.

RANSOMWARE – OS MEUS FICHEIROS FORAM RAPTADOS E AGORA?

COMO POSSO SER “INFETADO”?

The screenshot shows an email client window titled "Incoming Fax Report — Западноевропейская (ISO)". The email header includes "Incoming Fax (no-reply@send-efax.com)" and the date "18.03.2015 12:48". The recipient is listed as "fax-message942-7 58-273.zip".

Below the email, a file explorer window is open, showing the path "Administrator > Downloads > document-128_712". The file list contains one entry:

Name	Date modified	Type	Size
document-128_712.scr	30/06/2014 8:54 AM	Screen saver	138 KB

Below the file explorer, the email content is partially visible, showing "Line number: 7", "DTMF/DID:", and "Description: Internal only".



Email SPAM

COMO POSSO SER “INFETADO”?



Su paquete ha llegado a **20 de marzo**. 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 438685108339

[Descargar información sobre su envío](#)

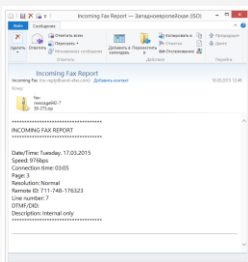
Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta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

Condiciones y T'erminos del Servicio de localización de envíos

La consulta del estado detallado para envíos individuales y del estado final para envíos masivos es un servicio gratuito que Correos le ofrece para sus envíos remitidos con carácter registrado. Este servicio es de carácter informativo sin que en ning'un caso sustituya la información que ud. puede obtener mediante acuse de recibo o certificación de servicios postales. Correos no se responsabiliza de los errores u omisión de información, por lo que advierte que no se adopten decisiones o acciones derivadas de la información obtenida por este servicio.

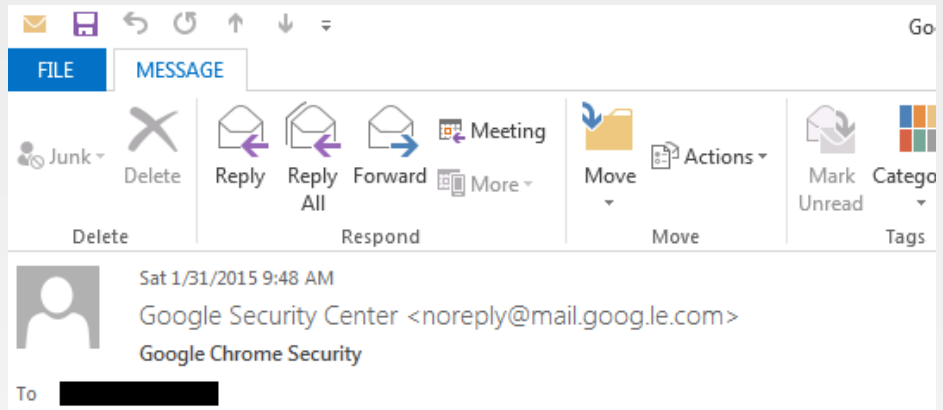
[Haga clic aquí para darse de baja.](#)

@ Copyright 2014 Sociedad Estatal Correos y Tel'grafos, S.A.



Email SPAM

COMO POSSO SER “INFETADO”?



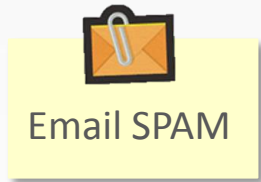
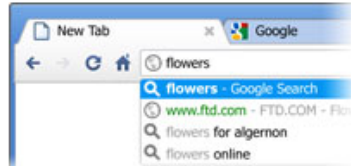
i If there are problems with how this message is displayed, click here to view it in a web browser.



Your version of Google Chrome is potentially vulnerable and out of date.


Download Google Chrome


It is **free** and installs in seconds
For Windows XP, Vista and 7



COMO POSSO SER “INFETADO”?

Bienvenidos | Benvidos | Benvinguts | Ongi etorri | Welcome













Hola, Identificate
Mi cuenta

Buscador >> Avanzado

Localizador >> Varios envíos

[ENVIAR DOCUMENTOS](#) |
 [ENVIAR PAQUETERÍA](#) |
 [SERVICIOS FINANCIEROS](#) |
 [FILATELIA](#) |
 [SERVICIOS ADICIONALES](#) |
 [SOLUCIONES EMPRESARIALES](#) |
 [INFORMACIÓN CORPORATIVA](#)

Estás en: [Inicio](#) | [Localizador de envíos](#)

Localizador individual

Para consultar el estado detallado de su **envío**, introduzca el código captcha y pulse "Consultar".

Código captcha:

2 2 5 5 8

Consultar

Atención al Cliente 902 197 197

197

Contacto

Guías de ayuda e información

Información corporativa

Acerca del Grupo Correos

RSC

Sala de prensa

Recursos humanos

Enlaces de interés

Museo Postal y Telegráfico

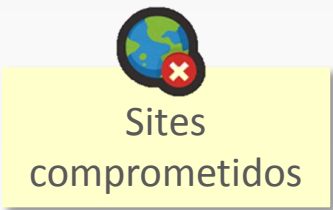
CorreosTelecom

Correos Express

Buscador >> Avanzado

Productos de la A a la Z

Lo más visitado



COMO POSSO SER “INFETADO”?

MALICIOUS ADVERTISING (“MALVERTISING”) IS A TYPE OF ONLINE ATTACK WHEREIN MALICIOUS CODE HIDDEN WITHIN AN ONLINE AD INFECTS YOUR COMPUTER WITH MALWARE.



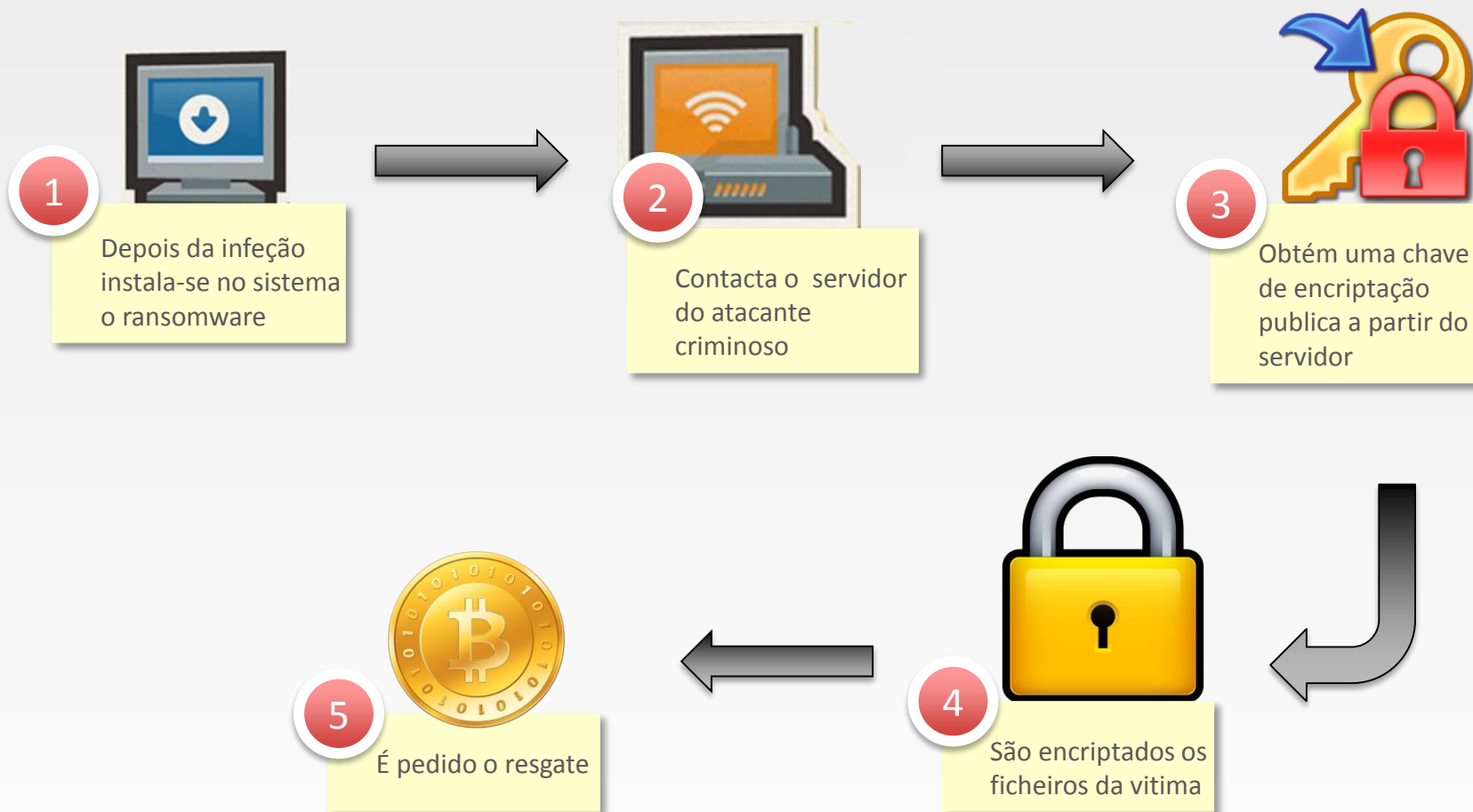
Sites comprometidos

COMO POSSO SER “INFETADO”?



SMS

COMO FUNCIONA O RAPTO?



COMO FUNCIONA O RAPTO?

Your personal files are encrypted by CTB-Locker.



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.



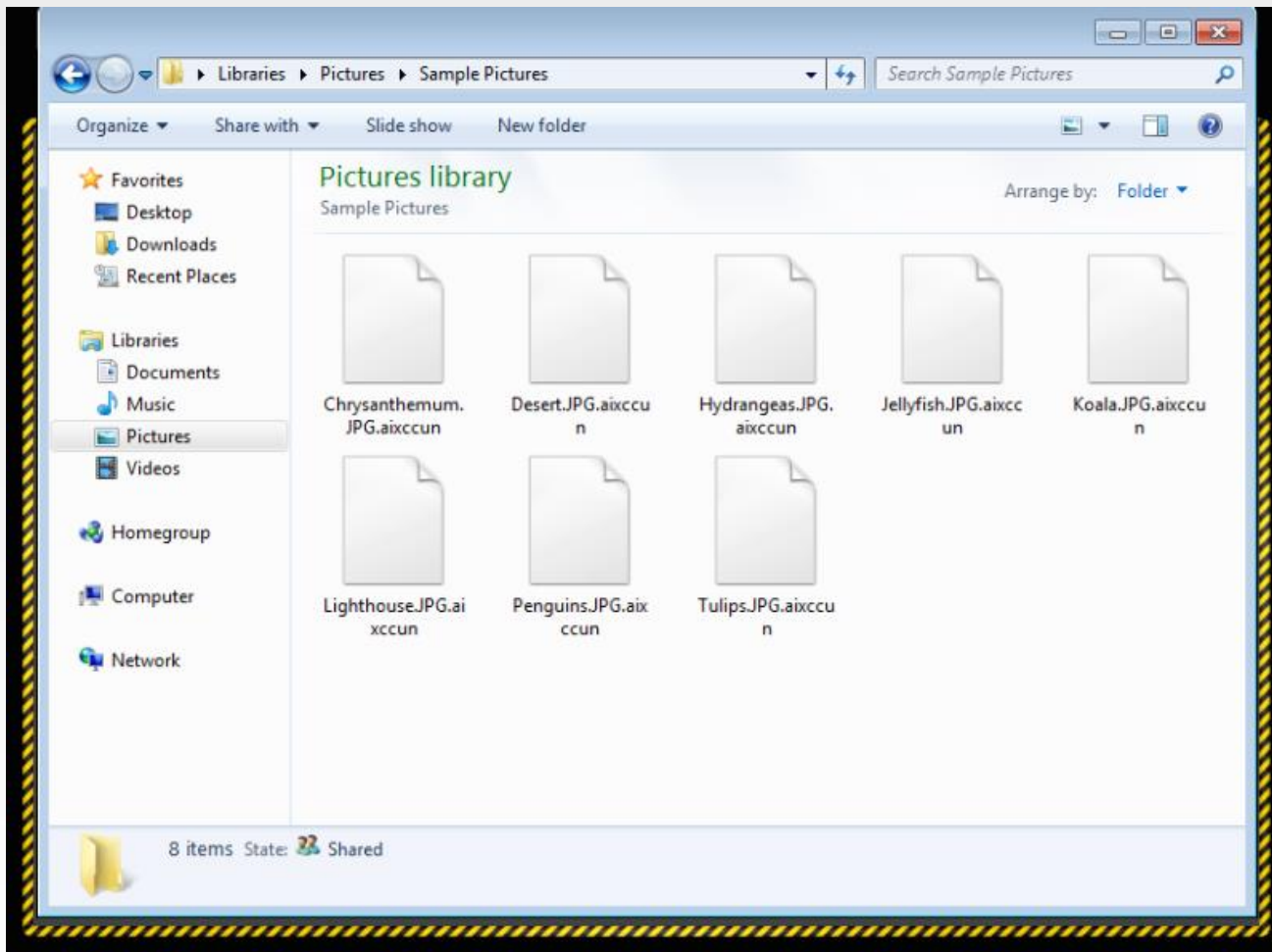
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View

95 59 50

Next >>

COMO FUNCIONA O RAPTO?



COMO FUNCIONA O RAPTO?

The image shows a ransomware interface with a dark background and a yellow and black striped border. At the top right, there is a small American flag icon. The main text is in red and white. Below the instructions, there are three yellow buttons: 'Search', '<< Back', and 'Next >>'. In the center, the time '71:36:53' is displayed in large yellow digits. The words 'SLEEPING COMPUTER' are faintly visible in the background.

Test decryption.

To make sure that decryption is possible you are allowed to decrypt up to 5 random files for free.

Press 'Search'. Program will scan your disks and decrypt several files.

Press 'Next' to connect to the secret server and decrypt all files.

Press 'Back' to go to the first page.

71:36:53

Search

<< Back

Next >>

COMO FUNCIONA O RAPTO?

Your personal files are encrypted by CTB-Locker.



Payment required.

Server accepts payment in Bitcoin (BTC) only.

1. Pay amount of 2 BTC (about of 500 USD) to address:

1H54arF71ayU3F6KuLrQE77iPq9j4dzfGt

2. Transaction will take about 15-30 minutes to confirm.

Decryption will start automatically. Do not: power off computer, run antivirus program, disable internet connection. Failures during key recovery and file decryption may lead to accidental damage on files.

If you have no Bitcoins press 'Exchange'.

95 57 08

Exchange >>

OS MEUS FICHEIROS FORAM RAPTADOS E AGORA?

Desligue o computador da rede

Desligue o computador da rede / internet, pois o ransomware pode estar a tentar infetar todas as partilhas de rede que encontra.

Restaure de um Backup

Não é possível descriptar os dados sem acesso à chave privada que está em posse do atacante. A solução é formatar o computador e repor os dados de um backup anterior ao rapto.

Pague o resgate

Caso não existam backups ou os mesmos tenham sido destruídos pelo ransomware, a última opção (não recomendada) é pagar o resgate. Isto sem a garantia de que irá de facto obter a informação...

NEGOCIAR O RESGATE - 😊

2015-04-13 10:25 GMT+01:00 RV vice.ricardo@gmail.com:
Alex,
Like I told you, this entity is a non profit organization. They do not have IT support and asked us for help. They help poor people survive. If you want to help us we will be much appreciated. If not, it's a huge problem for all the people who work here and also for all the people they help.
Regards, Ricardo

On 10.04.2015 21:45, RV wrote:
This is a big problem for us.. :-(

On 10.04.2015 19:59, RV wrote:
We don't have the money to pay. Please help.

2015-04-10 18:55 GMT+01:00 Alex Smith <allsecinfo1@gmail.com>:
You want help for free, right?

2015-04-10 17:43 GMT+01:00 Alex Smith <allsecinfo1@gmail.com>:
No money no help, sorry.
Bye

2015-04-14 16:16 GMT+01:00 Alex Smith <allsecinfo1@gmail.com>:
Hello.
Our minimal price is 2000USD and we can accept this from you.
Thanks

RANSOMWARE É UM NEGÓCIO

Alto Rendimento

Um Cyber Criminal pode com esquemas de ransomware atingir receitas anuais médias de **\$84100 USD** com um investimento de apenas \$5900 USD. Tudo isto com baixo risco!

Ransomware Kits

Um Cyber Criminal não precisa de ser um expert em informática. Pode comprar um KIT de ransomware e um Exploit Kit e começar de forma simples as operações.

Rede de Afiliados

Existe também na darkWEB ofertas de filiação em que o master recebe uma percentagem do resgate obtido pelo afiliado.

MANTENHA-SE SEGURO

Faça Backups Regulares

Calendarize backups à sua informação ou mantenha a mesma num local com o backup controlado pelo Departamento de TI da sua Empresa. Teste os Backups!

Peça Ajuda

Contacte o departamento de TI caso note atividade suspeita no seu computador. Não abra anexos em e-mails suspeitos!

Use Antimalware

É essencial um software de proteção com capacidade de identificar tráfego malicioso

Atualize o computador

Mantenha o computador com as últimas atualizações de segurança.

CONTACTOS

- DEPARTAMENTO COMERCIAL

// Daniel Oliveira

daniel.oliveira@knowledgeinside.pt

Tlm: 936 373 150

- DEPARTAMENTO TI

// Nuno Carvalho

nuno.carvalho@knowledgeinside.pt

Tlm: 936 036 863

- KNOWLEDGE INSIDE, LDA.

// Polo Tecnológico de Lisboa, Edifício 3
Estrada do Paço do Lumiar
1600-546 Lisboa

Telf.: 210 174 216 // Fax: 210 174 220

////////////////////
/

COMEÇE AGORA!
A TRABALHAR MAIS PARA O SEU NEGÓCIO
E MENOS PARA A TECNOLOGIA.



RANSOMWARE – EXTRAS – THE DARK SIDE

EXPLOIT KIT DASHBOARD

Blackhole ^β
Logout

Adv: Selling Iframe traffic in a huge amount JID#1: buldozer790@jabber.ru icq#1: 609347060 JID#2: technicalsupport911@jabber.org icq#2: 622729573
 Adv: IframeShop.net - comfortable buying\selling iframe traffic with no limits. 256 countries, 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.

Start date: End date: Apply Autoupdate interval: **10 sec.**

STATISTIC

TOTAL INFO 14.08%

43605 HITED 23249 HOSTS 3273 LOADS LOADS

TODAY INFO 14.01%

32645 HITED 18160 HOSTS 2543 LOADS LOADS

EXPLOITS ↓

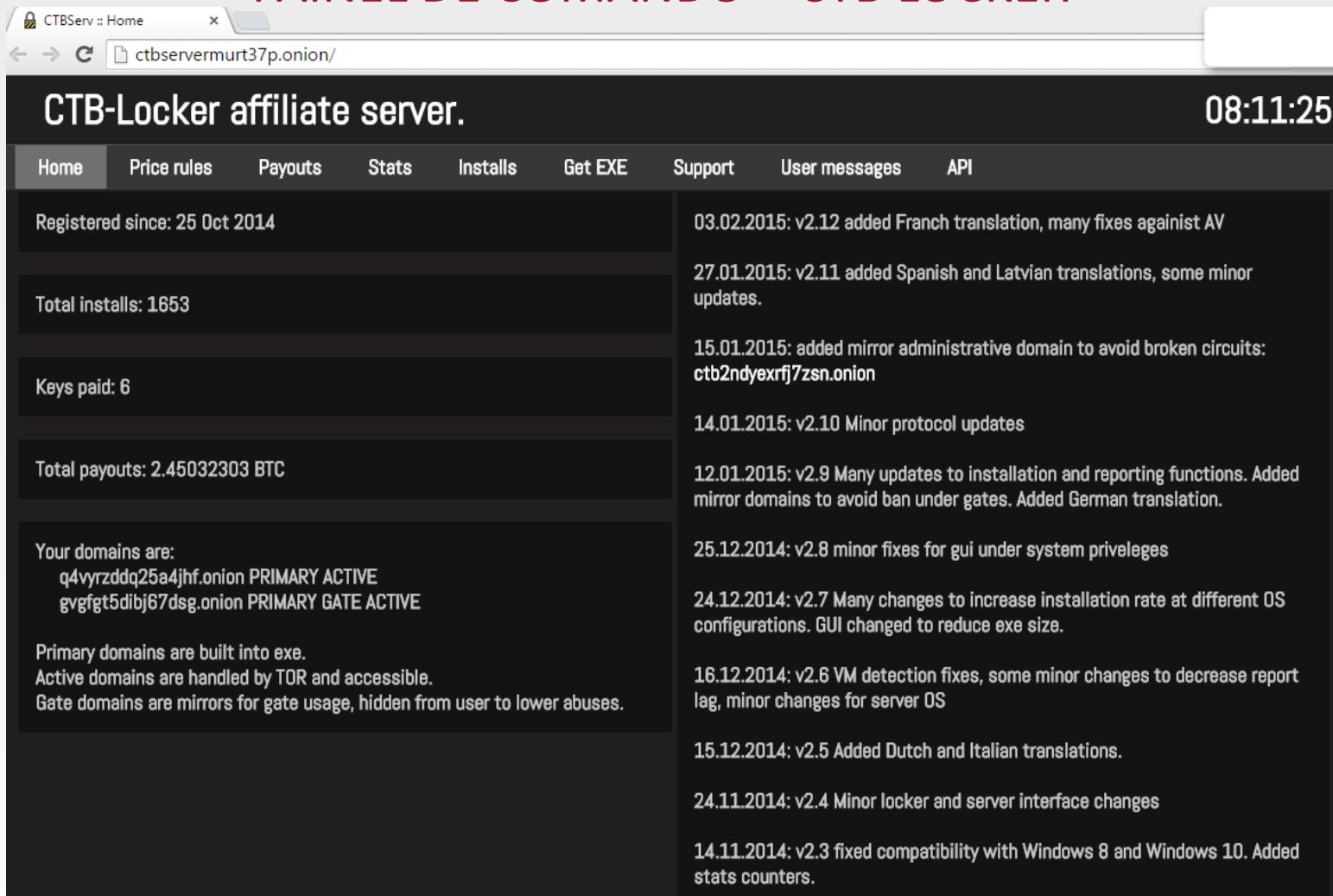
	LOADS	%
FLASH >	427	12.14 <input type="range" value="12.14"/>
HCP >	93	2.64 <input type="range" value="2.64"/>
JAVA SKYLINE >	168	4.78 <input type="range" value="4.78"/>
Java OBE >	1236	35.14 <input type="range" value="35.14"/>
Java SMB >	541	15.38 <input type="range" value="15.38"/>
MDAC >	65	1.85 <input type="range" value="1.85"/>
PDF ALL >	105	2.99 <input type="range" value="2.99"/>
PDF LIBTIFF >	882	25.08 <input type="range" value="25.08"/>

OS ↓	HITS	HOSTS	LOADS	%
Windows 7	20162	10843	740	6.82 <input type="range" value="6.82"/>
Windows Vista	1971	1160	206	17.76 <input type="range" value="17.76"/>
Windows XP	21479	12256	2410	19.68 <input type="range" value="19.68"/>

BROWSERS ↓	HITS	HOSTS	LOADS	%
Firefox >	11552	7208	1099	15.26 <input type="range" value="15.26"/>
MSIE >	10963	5838	1119	19.17 <input type="range" value="19.17"/>
Opera >	21090	11477	1164	10.14 <input type="range" value="10.14"/>

COUNTRIES ↑	HITS	HOSTS	LOADS	%
United States	16	3	0	0.00 <input type="range" value="0.00"/>
Russian Federation	43579	23243	3273	14.08 <input type="range" value="14.08"/>
Netherlands	3	1	0	0.00 <input type="range" value="0.00"/>
Germany	5	2	0	0.00 <input type="range" value="0.00"/>

PAINEL DE COMANDO – CTB LOCKER



CTBServ :: Home x

ctbservermurt37p.onion/

CTB-Locker affiliate server. 08:11:25

[Home](#)
[Price rules](#)
[Payouts](#)
[Stats](#)
[Installs](#)
[Get EXE](#)
[Support](#)
[User messages](#)
[API](#)

<p>Registered since: 25 Oct 2014</p> <hr/> <p>Total installs: 1653</p> <hr/> <p>Keys paid: 6</p> <hr/> <p>Total payouts: 2.45032303 BTC</p> <hr/> <p>Your domains are: q4vyrzddq25a4jhf.onion PRIMARY ACTIVE gvfgt5dibj67dsg.onion PRIMARY GATE ACTIVE</p> <p>Primary domains are built into exe. Active domains are handled by TOR and accessible. Gate domains are mirrors for gate usage, hidden from user to lower abuses.</p>	<p>03.02.2015: v2.12 added Franch translation, many fixes against AV</p> <p>27.01.2015: v2.11 added Spanish and Latvian translations, some minor updates.</p> <p>15.01.2015: added mirror administrative domain to avoid broken circuits: ctb2ndyexrfj7zsn.onion</p> <p>14.01.2015: v2.10 Minor protocol updates</p> <p>12.01.2015: v2.9 Many updates to installation and reporting functions. Added mirror domains to avoid ban under gates. Added German translation.</p> <p>25.12.2014: v2.8 minor fixes for gui under system priveleges</p> <p>24.12.2014: v2.7 Many changes to increase installation rate at different OS configurations. GUI changed to reduce exe size.</p> <p>16.12.2014: v2.6 VM detection fixes, some minor changes to decrease report lag, minor changes for server OS</p> <p>15.12.2014: v2.5 Added Dutch and Italian translations.</p> <p>24.11.2014: v2.4 Minor locker and server interface changes</p> <p>14.11.2014: v2.3 fixed compatibility with Windows 8 and Windows 10. Added stats counters.</p>
--	--

PAINEL DE COMANDO – CTB LOCKER

CTB-Locker affiliate server. 08:20:25

Home Price rules Payouts Stats Installs Get EXE Support User messages API

No rules defined

Country code in list: * and SubID=* and Size>0 Mb or files => Price:

Comment:

Default unlock price in BTC:

Default price is used when no rule matches.
0.6 BTC = 138 USD. Your affiliate reward is 0.42 BTC = 96 USD

PAINEL DE COMANDO – CTB LOCKER

CTB-Locker affiliate server.
08:22:25

Home
Price rules
Payouts
Stats
Installs
Get EXE
Support
User messages
API

Use mixing services to clean all received money.

Payout addresses:

1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ del

Your BTC address: Add

Payout history:

N	Time	Installation ID	SubID	Address	Txid	Sum
1	30/10 04:58	5e2f198e4b42940d	0	1KivXueuzNzWgSKwRZ.JnS3eAoRtttgcLKg	9e4c17c49548cb88e46c375c34c2a4eoad2a3ddcfd8cde776c9f1f06810906e	0.35
2	07/11 06:19	e89964c7d3427395	31	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	f6d73ff4001f87c8968f180ad8fa9e9fe569872bb59a883c3fd522d5930f711	0.42
3	12/11 14:55	1b4980440d4dc12e	1211	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	490e3a5934a559b7aa0c919b1b5d78777bc2e2df2625bfd025d3d89ca18ff275	0.42
4	14/11 12:48	cbb42ba8414d003f	1211	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	a00bbeff1ef18c21c8b930746de8e1938029f20462e1e71b0460e94461272bbcd	0.42
6	27/11 17:04	8ea2fb362041b1eb	2211	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	cf05b4056d1fcb766e19db65a29a1e9b492cf6d4c5caca8b4ea4953596cbb1c	0.42032303
6	08/01 15:13	c40b7217f948e4b6	1209	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	7625caab87767f9f24093786b30043d3b3d83e503509b6bfc7eb7ff13b16c00	0.42

Payouts by SubID:

SubID	Sum	Count
0	0.35	1
31	0.42	1
1209	0.42	1
1211	0.84	2
2211	0.42032303	1

PAINEL DE COMANDO – CTB LOCKER

CTB-Locker affiliate server.
08:24:25

Home
Price rules
Payouts
Stats
Installs
Get EXE
Support
User messages
API

Show all

SubID	Count
0	254
22	4
31	102
1209	134
1211	407
1311	282
1411	126
1511	154
2211	190

N	Reported	Last active	Installation ID	Mode	V	OS	CC	TZ	Geo	SubID	Files	Address for payment	Price	Paid
1630	10/12 15:20	08/01 15:18 W	c40b7217f948e4b6	GUI	2.4	6.1.x64 H	TW	+8	TW	1209	8=0MB	1962N5WXpaXNo8p5CXCYXNFRkG3nkiB5aM	0.6	0.6
1468	24/11 10:59	27/11 17:08 WD	8ee2fb362041b1eb	GUI	2.3	5.1	PL	+1	PL	2211	7946=44.5GB	1ExApRqrCyn4eMV58sj48TChp1zzWtzS2	0.6	0.60046147
434	12/11 00:44	12/11 17:07 N	1b4960440d4dc12e	GUI	2.2	5.1	AU	+10	AU	1211	53827=19.9GB	1KdeqBij3erwtFSDDC8Pa9KLT2KztD9rRf	0.6	0.6
410	11/11 23:54	14/11 12:50 WD	cbb42be8414d003f	GUI	2.2	6.2.Srv	PT	+0	PT	1211	34797=30.9GB	1KfoI8B5GZK3x9qtfPecVob2kwPt4syNdV	0.6	0.6
341	02/11 09:29	07/11 05:21 WD	e89964c7d3427395	GUI	2.2	6.1.x64 H		+8	TW	31	821=30.3GB	1Hc8GwI6AbB3GItY2I4ND8GeoEb9Nmm3j	0.6	0.6
152	29/10 18:49	30/10 05:15 W	5e2f198e4b42940d	WEB	2.2	6.1.x64 H		+8	TW	0		1BY2MsK9RCJtwU3aipD56BC8Qx4oKdhQQcm	0.5	0.5

Last active hints:

- G - GUI with direct TOR connection
- N - NoTOR or GUI via tor2web proxy
- W - manual webpage via Tor Browser
- D - decoded test file via Tor Browser

OS hints:

- L - Low integrity level.
- M - medium/user level
- H - high/admin/system level
- V - virtual machine. Usually bad/AV with exception of VDS

PAINEL DE COMANDO – CTB LOCKER

CTB-Locker affiliate server.

Home
Price rules
Payouts
Stats
Installs
Get EXE
Support
User messages
API

SubID: Get GUI locker ~660Kb

SubID: Get NoTOR locker ~140Kb

SubID - any number between 0 and 65535. You can use SubID to sort traffic or select price.

GUI Locker: original locker with GUI and TOR. Encrypts files, shows dialog and connect to the server via native TOR and TOR gate. Best load/install ratio because of using all available connection options.

NoTOR Locker: locker with GUI and TOR via gates. No TOR library inside. May have problems with connecting to the server due to unavailable gates.

Warning! Locker does not elevate privileges from IE Protected Mode (low process privileges). Use loader with low privilege exploit. Use FUD crypt before spread. Everytime get new exe from the server.

Make sure that your exe cryptor supports running under system and local service account without .NET and GUI. Falling under system will cause lower installation rate. Before installs test your cryptor for 3 cases: XPx32, 7x32, 7x64. Rollback to clean OS before testing. Locker does not installs twice

PAINEL DE COMANDO – CTB LOCKER

CTB-Locker affiliate server.

[Home](#)

[Price rules](#)

[Payouts](#)

[Stats](#)

[Installs](#)

[Get EXE](#)

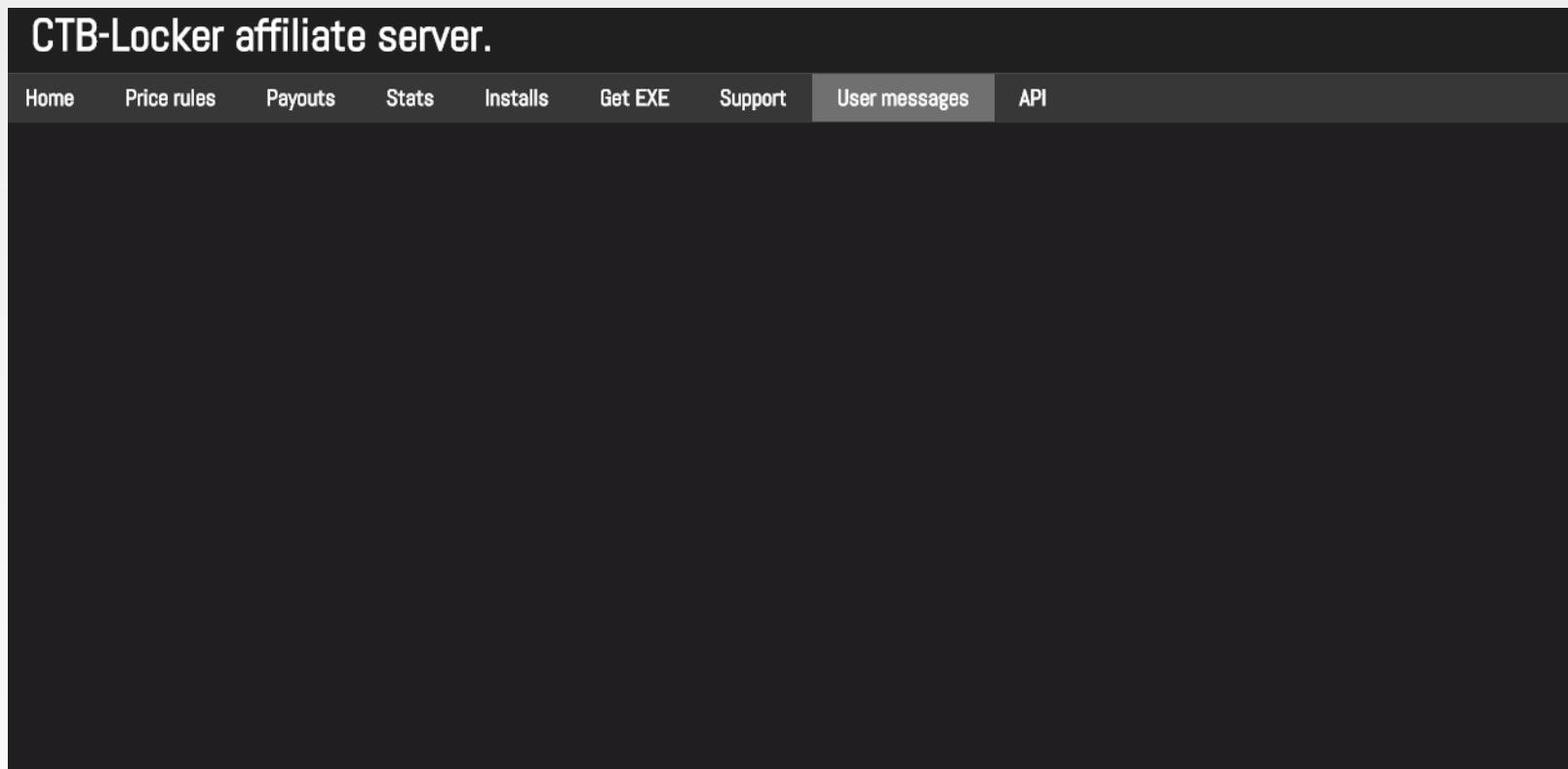
[Support](#)

[User messages](#)

[API](#)

Send

PAINEL DE COMANDO – CTB LOCKER



PAINEL DE COMANDO – CTB LOCKER

CTB-Locker affiliate server.

[Home](#)[Price rules](#)[Payouts](#)[Stats](#)[Installs](#)[Get EXE](#)[Support](#)[User messages](#)[API](#)

Payouts report:

<http://ankb65heu3x62dwb.onion/8vscl0emqk5dg6r2ay/payouts.xml> - full list

Installs report:

<http://ankb65heu3x62dwb.onion/8vscl0emqk5dg6r2ay/installs.xml> - full list (not recommended)

<http://ankb65heu3x62dwb.onion/8vscl0emqk5dg6r2ay/installs.xml?from=N&last=TIME&fields=XXXX> - filtered list

from=N - filter list by starting number, default N=0

last=TIME - filter list by last time (unix format), default N=0

fields=XXXXX - decimal bitmask value to select fields in output. default and 0 means all fields.