
KNOWLEDGE
INSIDE
www.knowledgeinside.pt
MAKE IT MORE VALUABLE

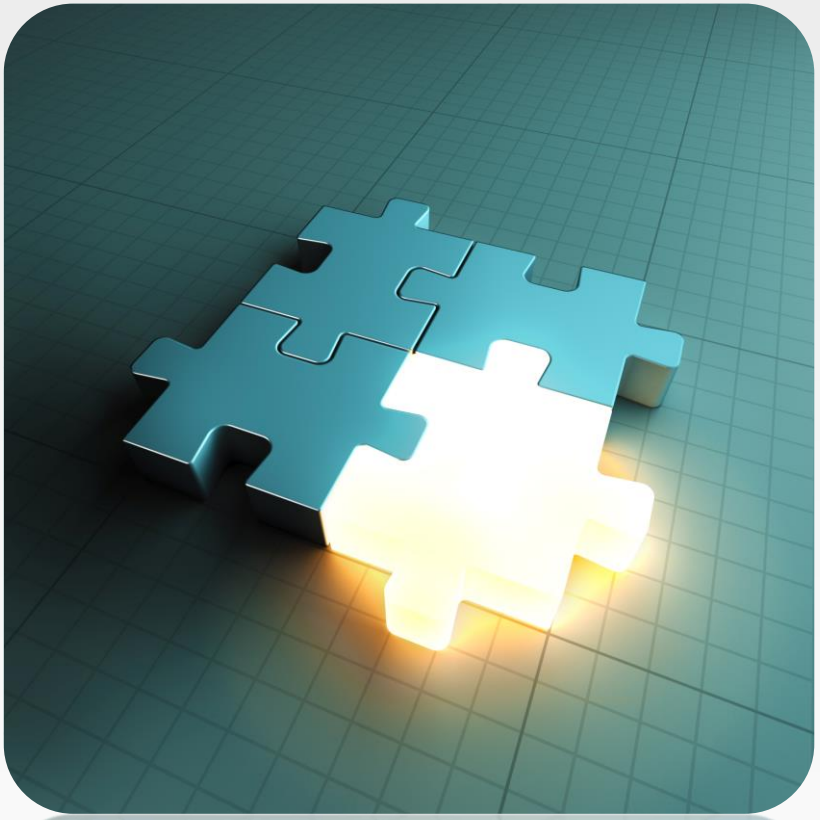
SOBRE A KNOWLEDGE INSIDE

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



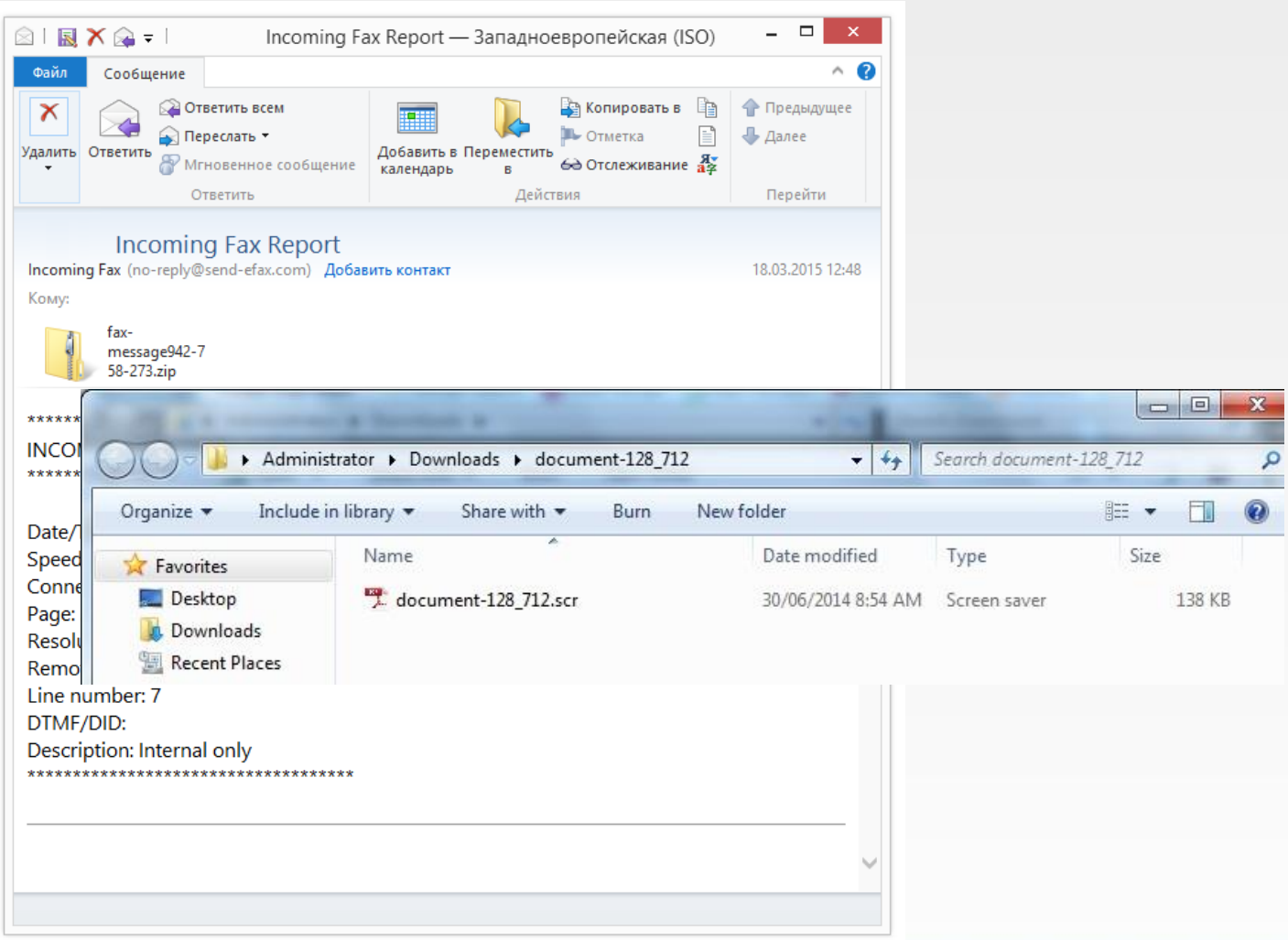
RANSOMWARE – OS MEUS FICHEIROS FORAM RAPTADOS E AGORA?

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 criticas do sistema ou em alguns casos a todo o computador. Para recuperar o acesso aos ficheiros ou ao sistema é exigido à vitima que **pague um resgate.**

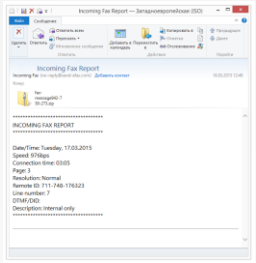
RANSOMWARE – OS MEUS FICHEIROS FORAM RAPTADOS E AGORA?

COMO POSSO SER “INFETADO”?



Email SPAM

COMO POSSO SER “INFETADO”?



Email SPAM

CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

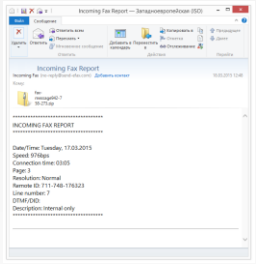
Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

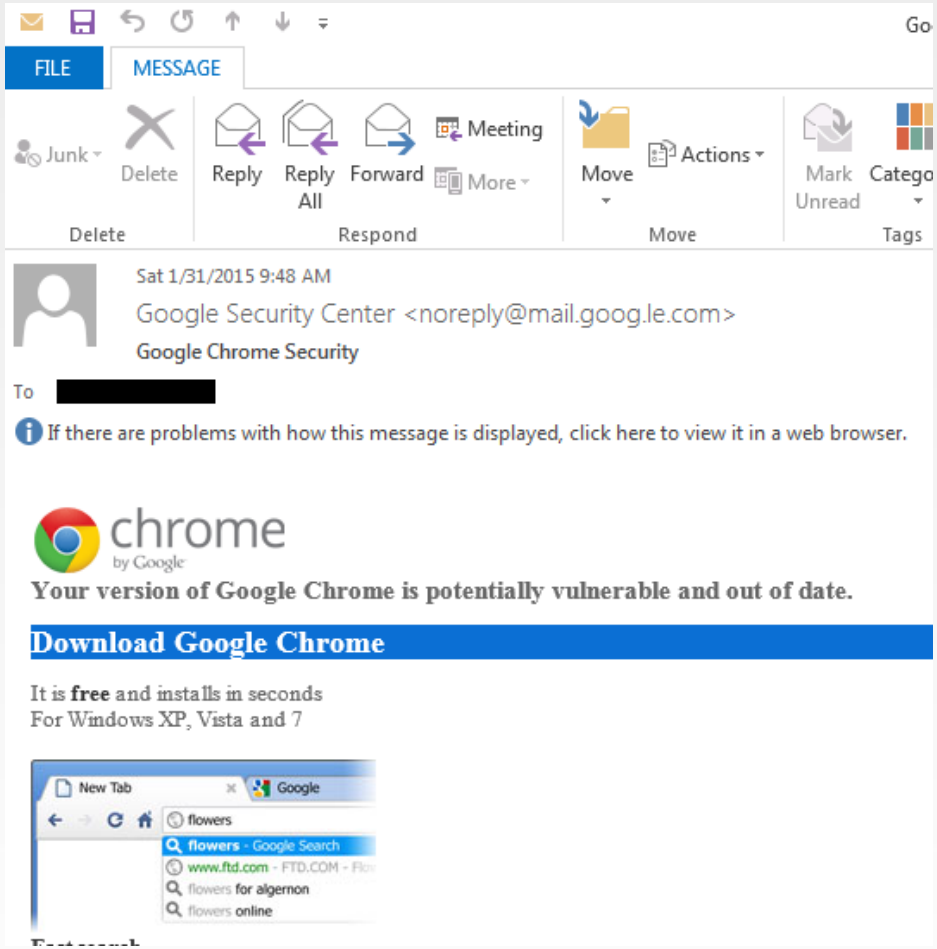
La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede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

Haga clic aqu'i para darse de baja.

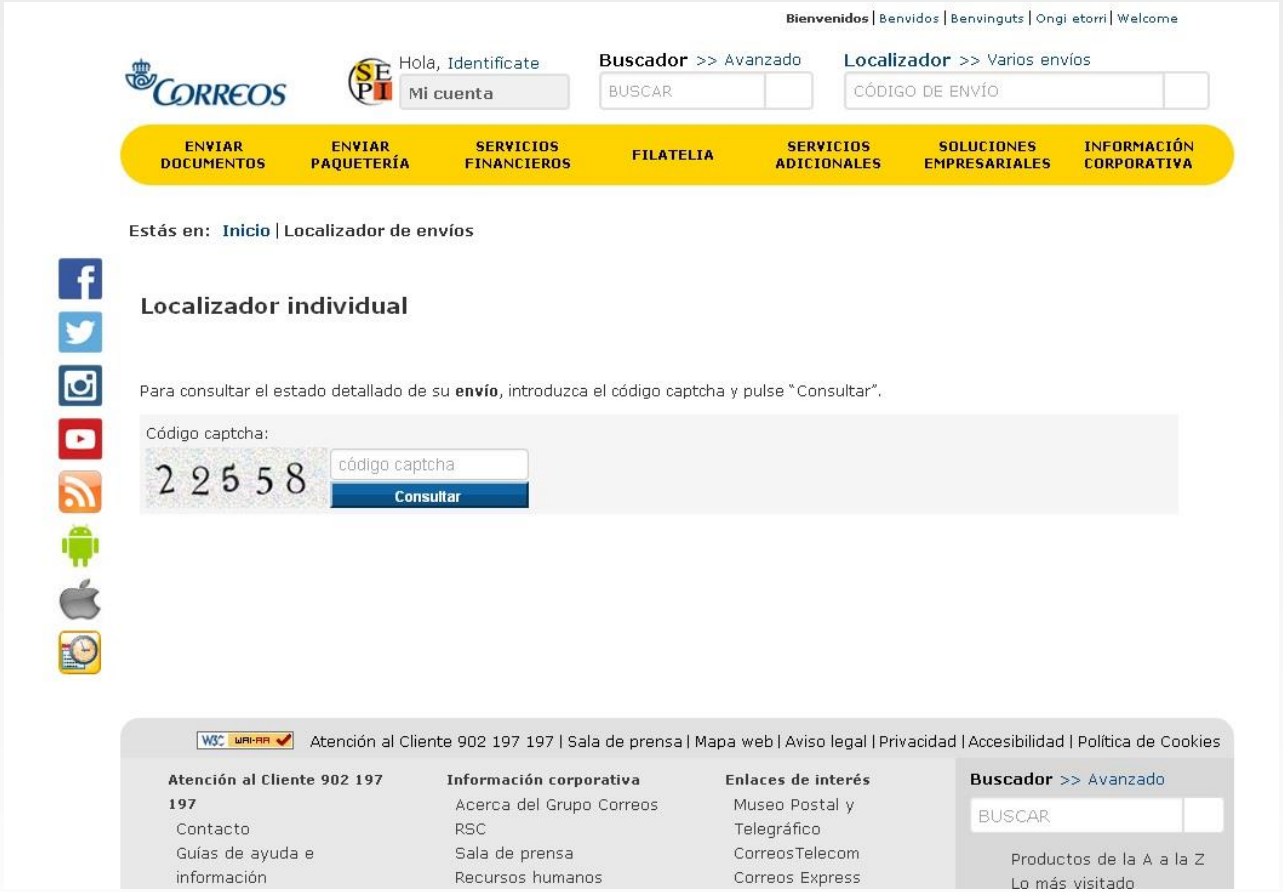
COMO POSSO SER “INFETADO”?



Email SPAM



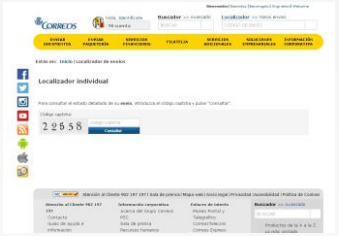
COMO POSSO SER “INFETADO”?



Sites comprometidos

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?

1. Depois da infeção instala-se no sistema o ransomware

2. Contacta o servidor do atacante criminoso

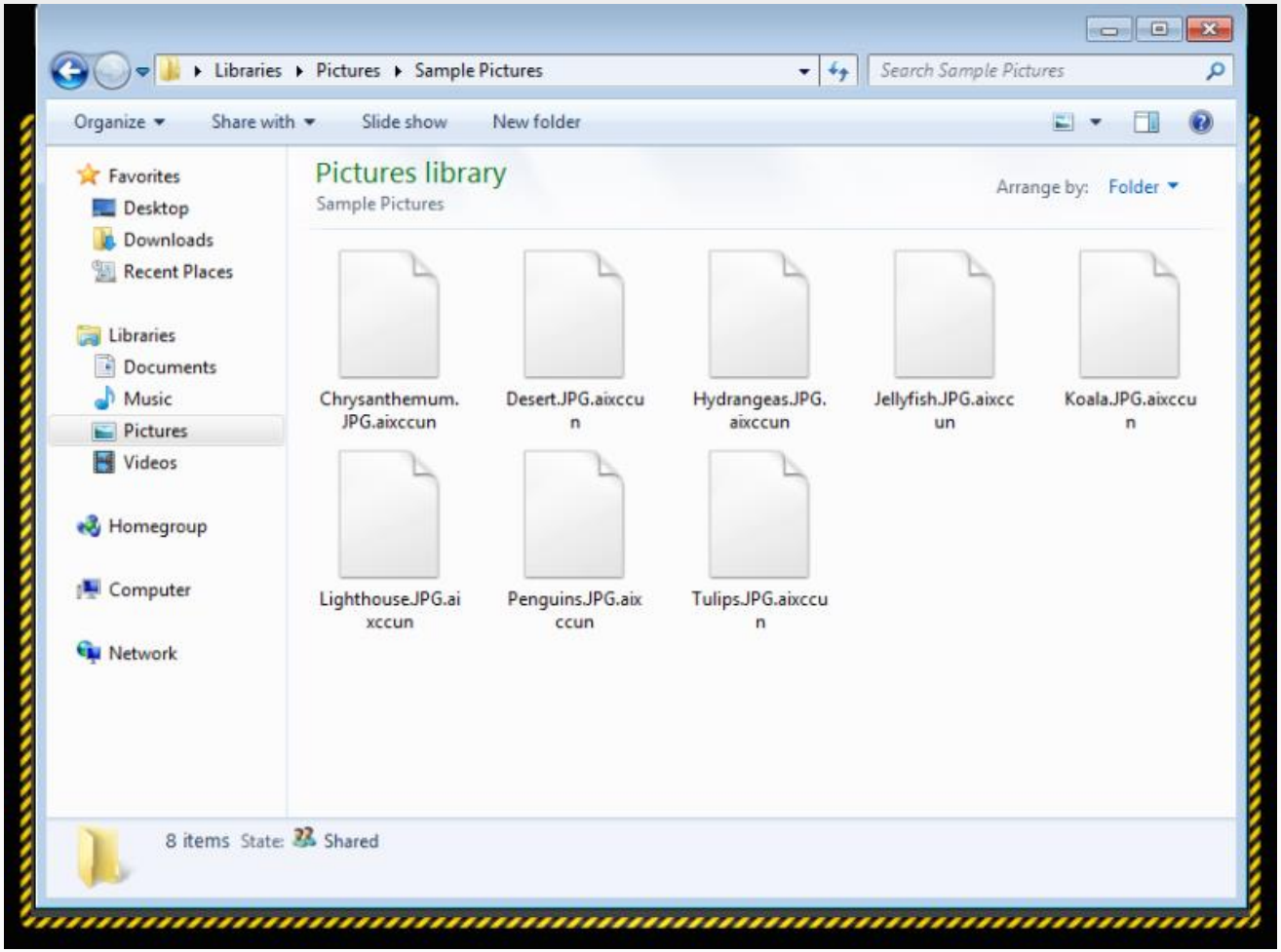
3. Obtém uma chave de encriptação publica a partir do servidor

4. São encriptados os ficheiros da vitima

5. É pedido o resgate

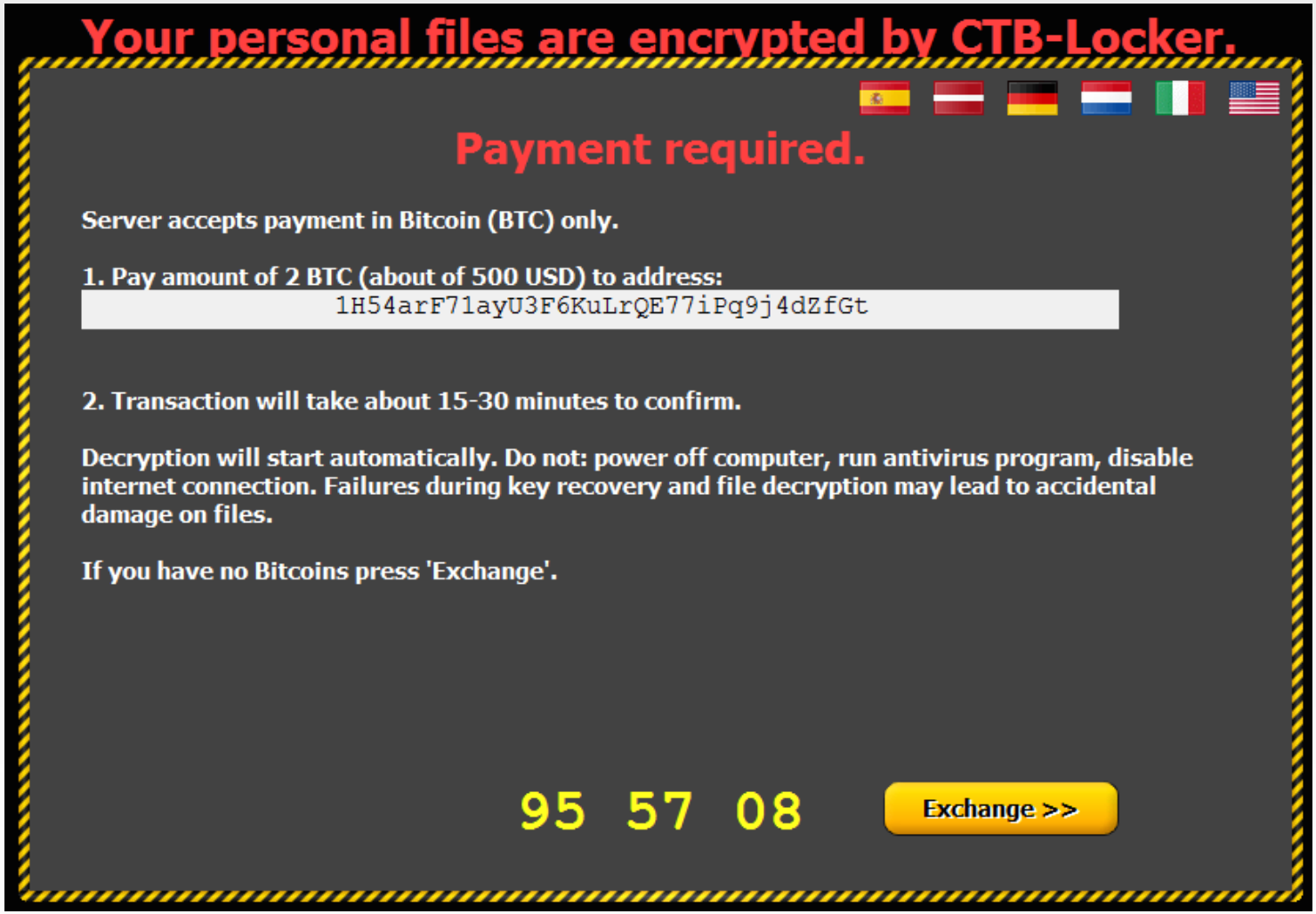
COMO FUNCIONA O RAPTO?

COMO FUNCIONA O RAPTO?



COMO FUNCIONA O RAPTO?

COMO FUNCIONA O RAPTO?



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 desencriptar 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 afilado.

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.

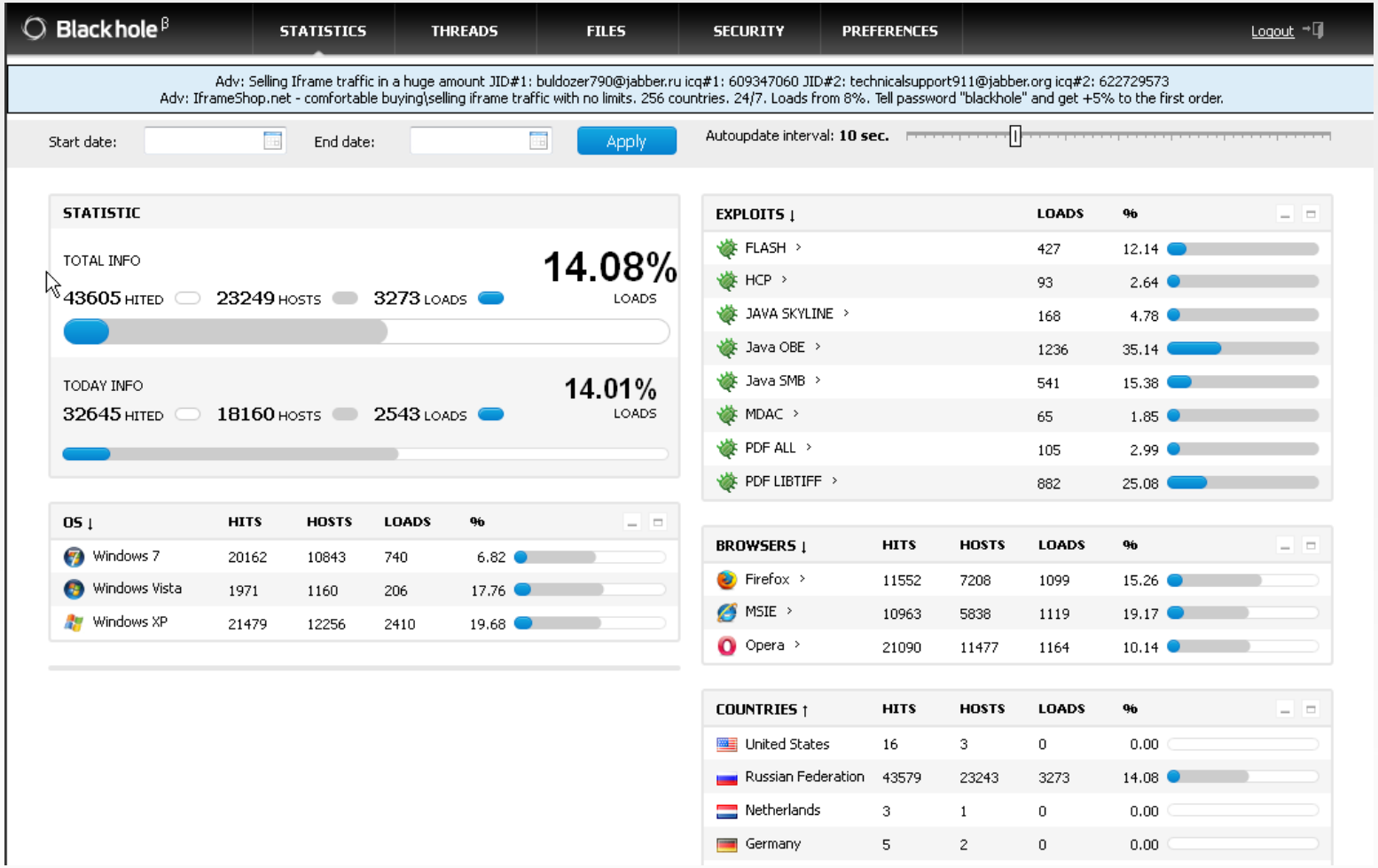
// Polo Tecnológico de Lisboa, Edifício 3
Estrada do Paço do Lumiar
1600-546 Lisboa

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

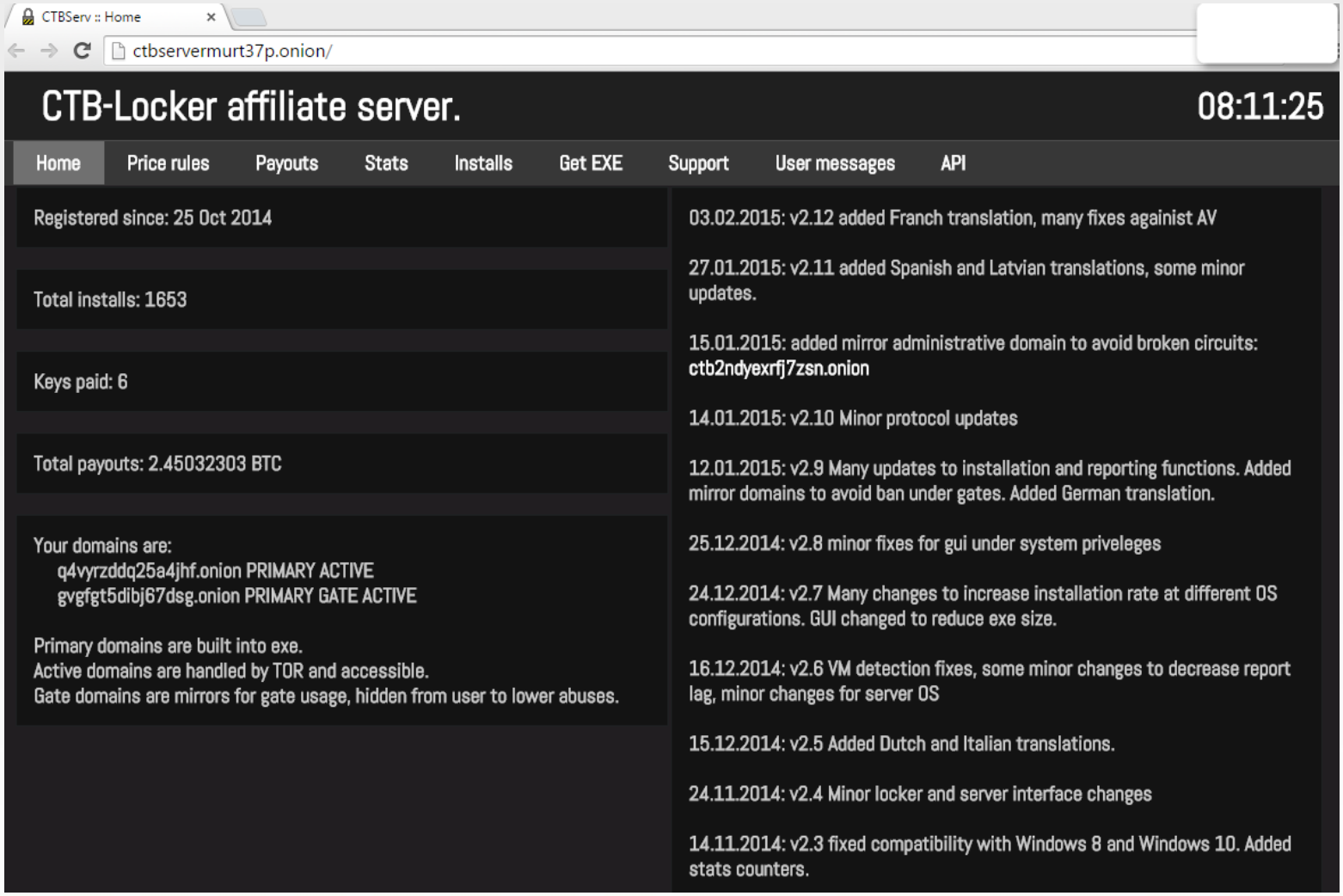
COMEÇE AGORA!
A TRABALHAR MAIS PARA O SEU NEGÓCIO
E MENOS PARA A TECNOLOGIA.

RANSOMWARE – EXTRAS – THE DARK SIDE

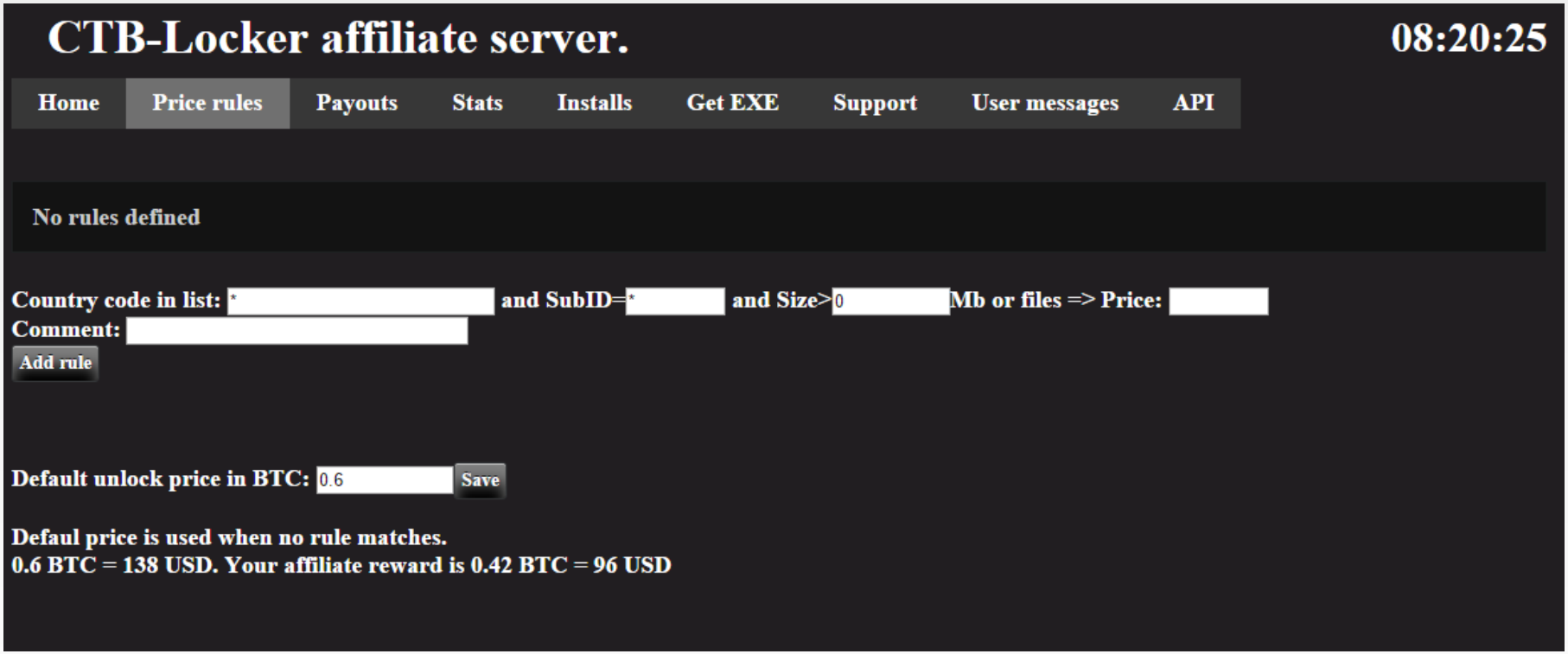
EXPLOIT KIT DASHBOARD



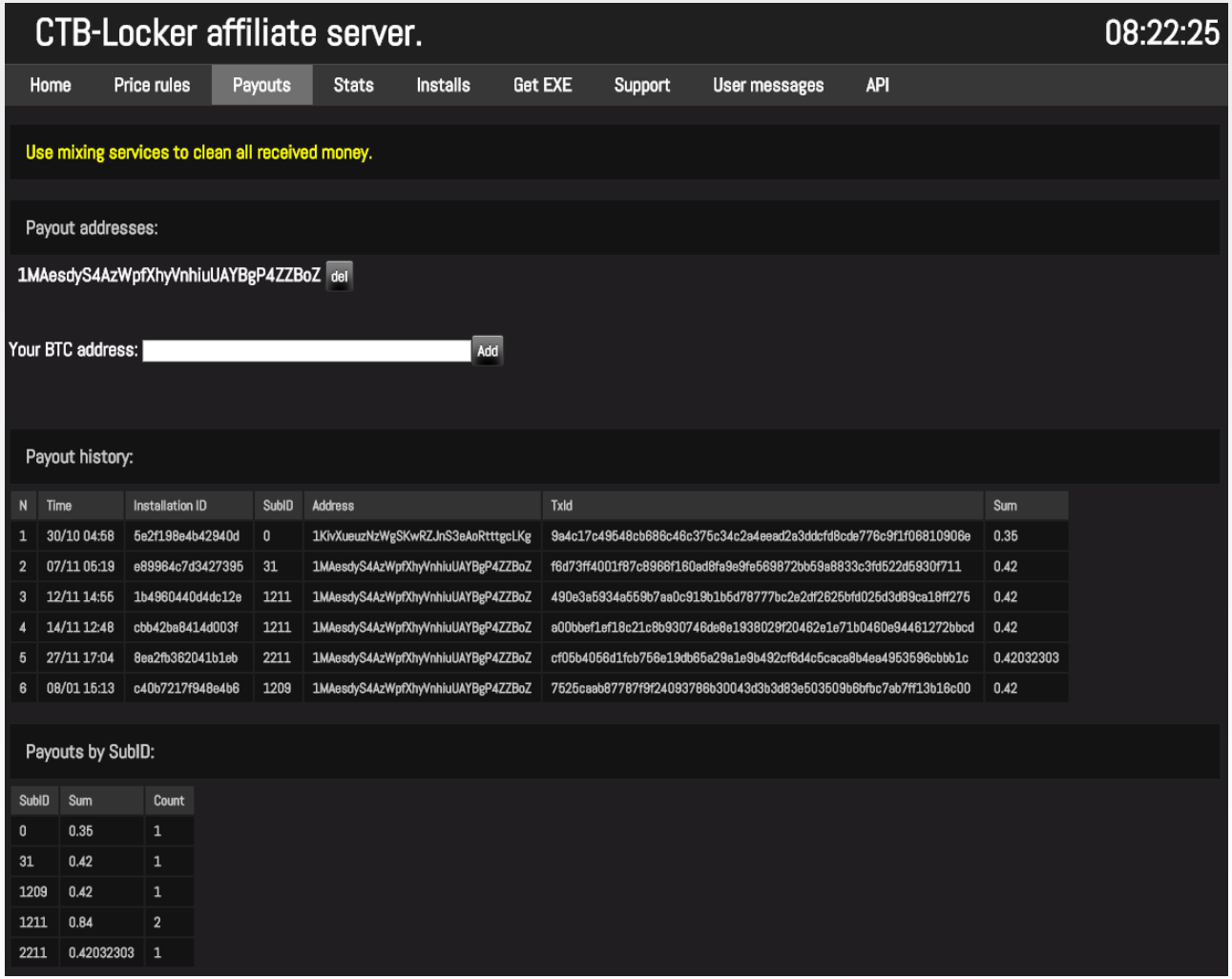
PAINEL DE COMANDO – CTB LOCKER



PAINEL DE COMANDO – CTB LOCKER



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

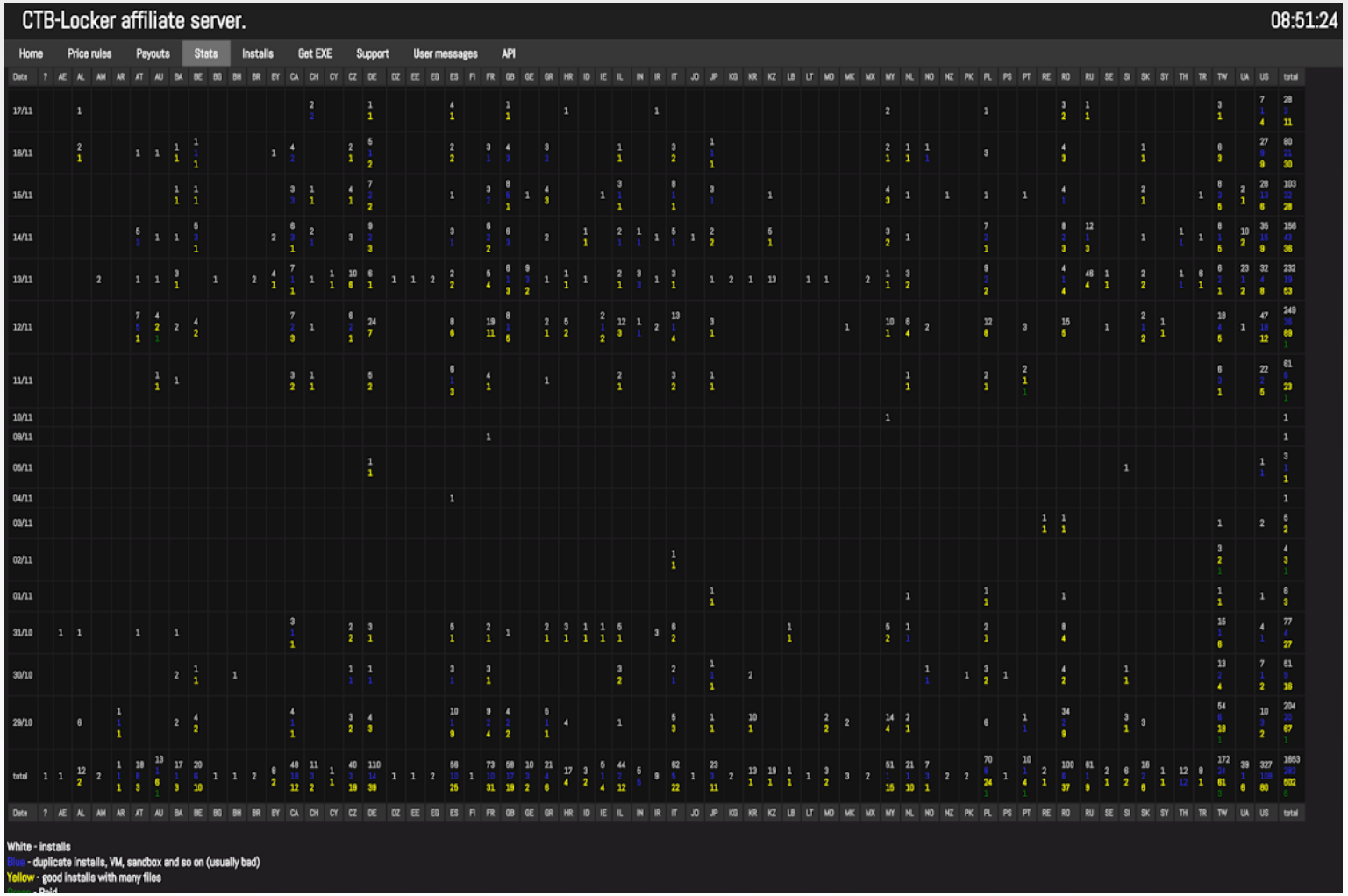
Payout history:

N	Time	Installation ID	SubID	Address	TxId	Sum
1	30/10 04:58	5e2f198e4b42940d	0	1KivXueuzNzWgSKwRZJnS3eAoRtttgcLKg	9a4c17c49548cb686c46c375c34c2a4eead2a3ddcfd8cde776c9f1f06810906e	0.35
2	07/11 05:19	e89964c7d3427395	31	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	f6d73ff4001f87c8968f160ad8fa9e9fe569872bb59a8833c3fd522d5930f711	0.42
3	12/11 14:55	1b4960440d4dc12e	1211	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	490e3a5934a559b7aa0c919b1b5d78777bc2e2df2625bfd026d3d89ca18ff275	0.42
4	14/11 12:48	cbb42ba8414d003f	1211	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	a00bbef1ef18c21c8b930746de8e1938029f20462e1e71b0460e94461272bbcd	0.42
5	27/11 17:04	8ea2fb362041b1eb	2211	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	cf05b4056d1fcb756e19db65a29a1e9b492cf6d4c5caca8b4ea4953596cbbb1c	0.42032303
6	08/01 15:13	c40b7217f948e4b6	1209	1MAesdyS4AzWpfXhyVnhiuUAYBgP4ZZBoZ	7525caab87787f9f24093786b30043d3b3d83e503509b6bfbc7ab7ff13b16c00	0.42

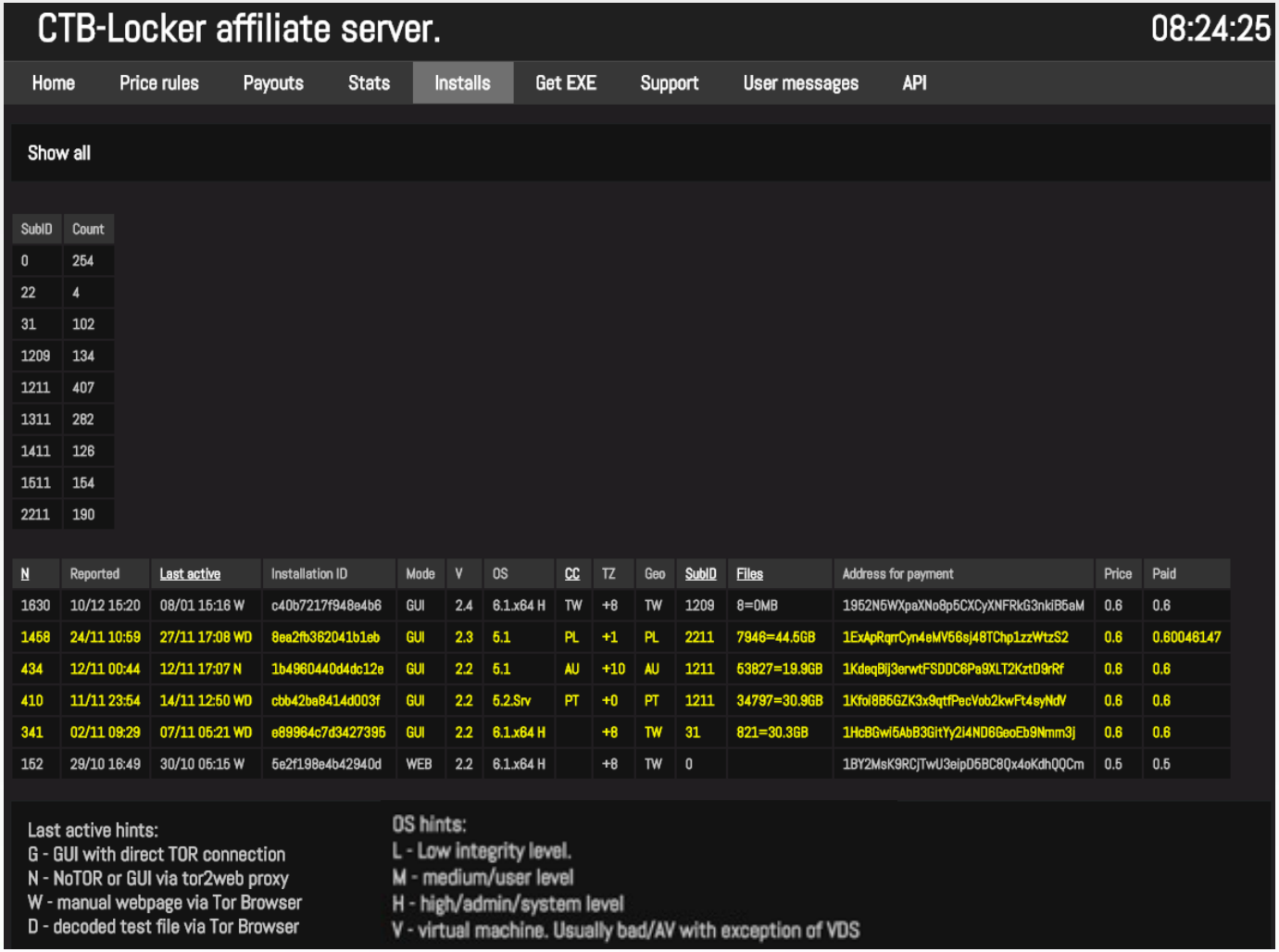
Payouts by SubID:

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

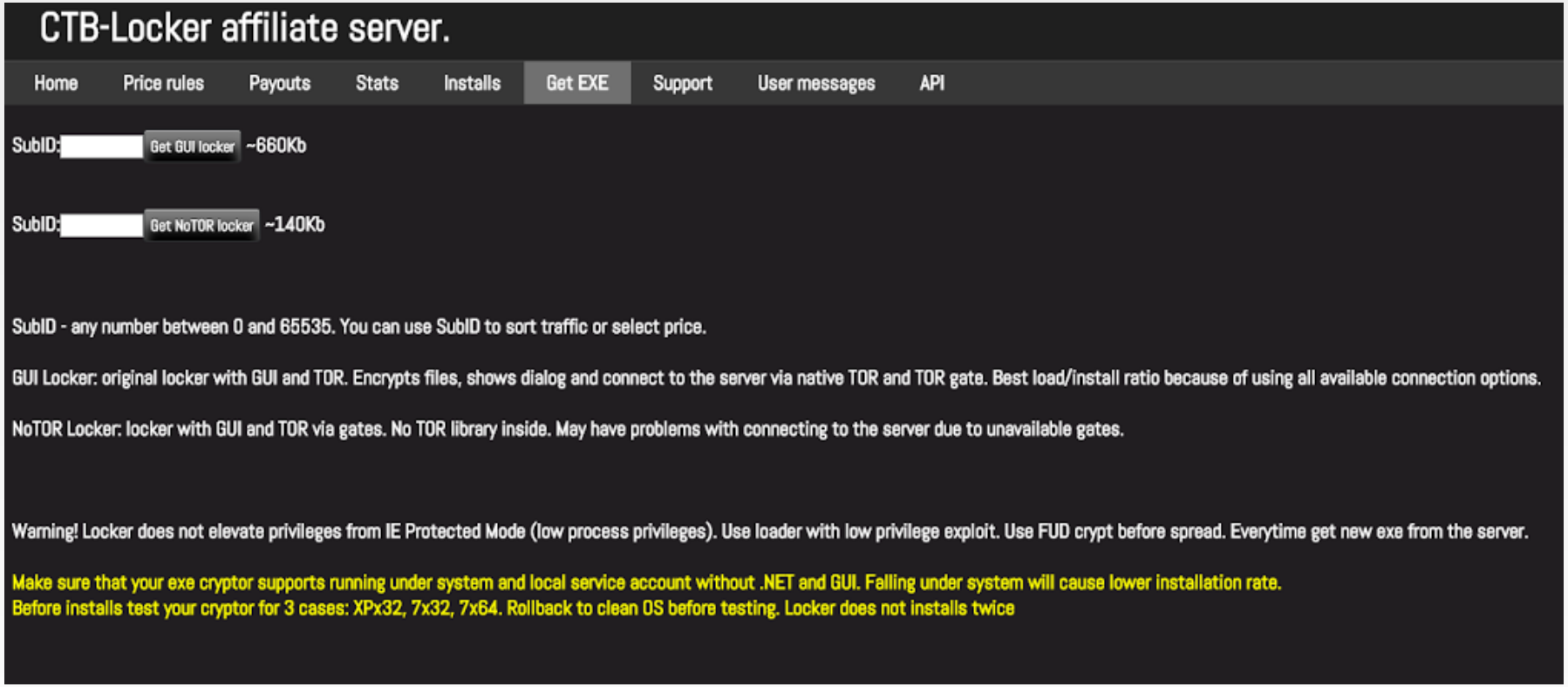
PAINEL DE COMANDO – CTB LOCKER



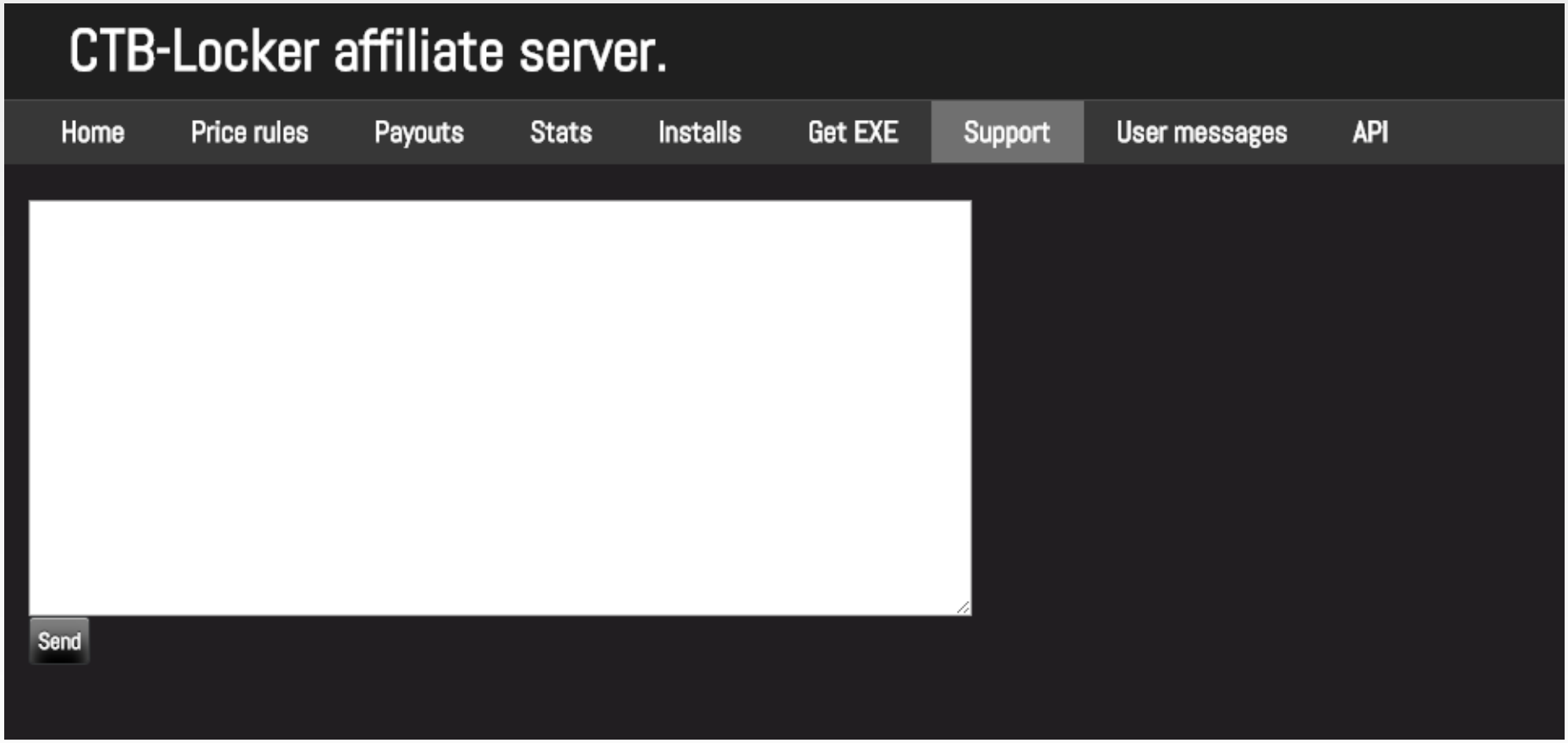
PAINEL DE COMANDO – CTB LOCKER



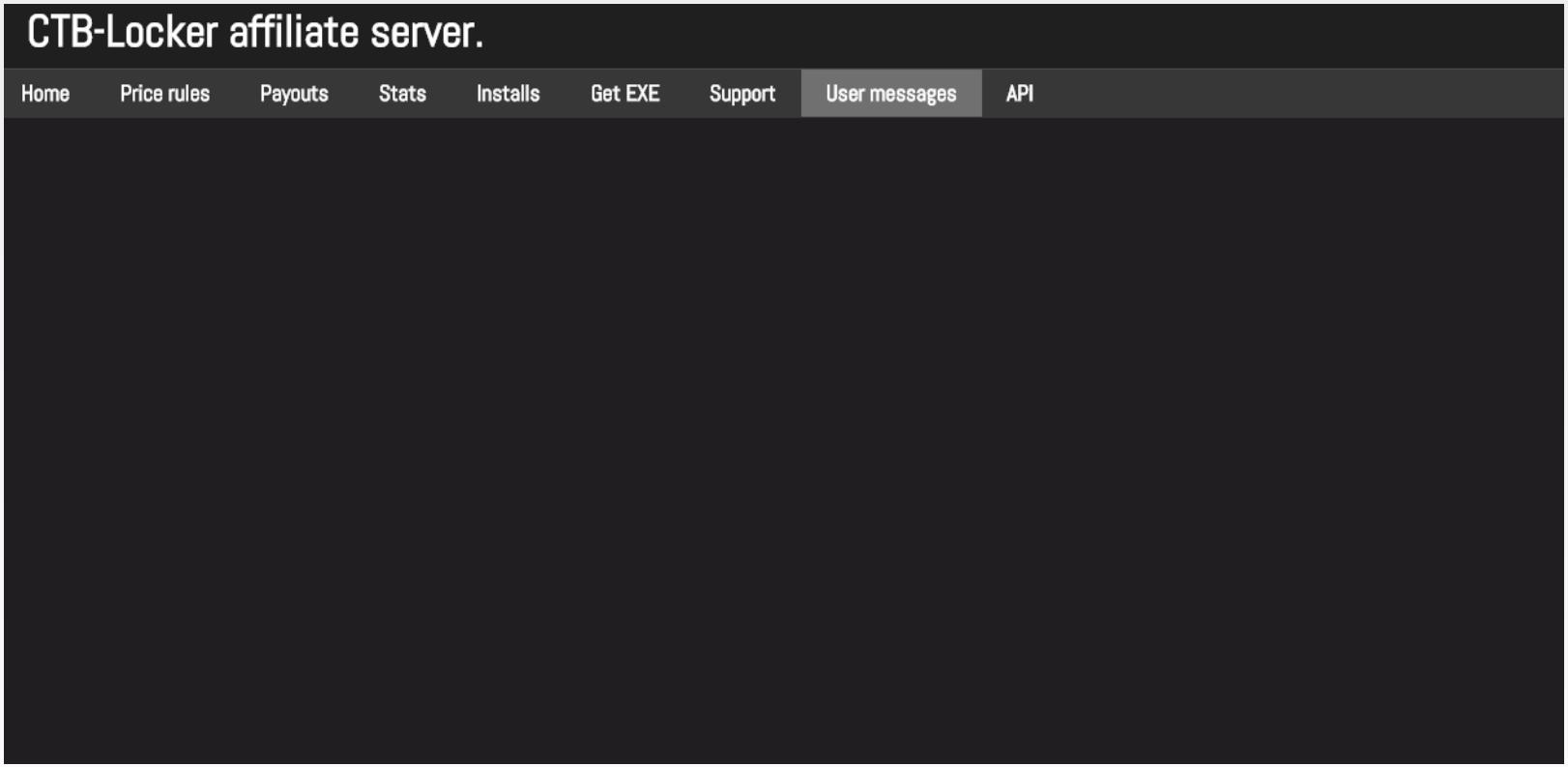
PAINEL DE COMANDO – CTB LOCKER



PAINEL DE COMANDO – CTB LOCKER



PAINEL DE COMANDO – CTB LOCKER



PAINEL DE COMANDO – CTB LOCKER