

# aenigma

The | state-of-the-art | secure-by-default | one-touch-deployed | XMPP server for everyone.



<https://aenigma.xyz>

# lo stato attuale dei servizi di IM

Signal



Pro:

- open source
- crypto state of the art
- audited and reviewed
- truly multi-client
- multi-client basato su key-exchange

Contro:

- centralizzato

# lo stato attuale dei servizi di IM

## WhatsApp



### Pro:

- *in teoria* implementa libaxolotl [signal]
- crypto state of the art [vedi #1]
- audited and reviewed [vedi #1]
- pseudo-mc basato su key-exchange

### Contro:

- centralizzato
- closed source
- pseudo-multiclient
  - Facebook

# lo stato attuale dei servizi di IM

## Telegram



### Pro:

- parzialmente open source
- multiclient ma non sulle chat E2EE
- funzioni client cool e hipster

### Contro:

- centralizzato
- backend closed source
- chat E2EE non multiclient
- E2EE meno rinomata rispetto a Signal

# lo stato attuale dei servizi di IM

WeChat





**E CORP**

# lo stato attuale dei servizi di IM

WeChat



Pro:

- SRSLY?

Contro:

- <integer overflow !@#\$%^&\*...>

# lo stato attuale dei servizi di IM

Status.IM



Note:

- Basato sulla blockchain di ethereum



# lo stato attuale dei servizi di IM

Ring.CX



Note:

- openDHT
- gnuTLS
- database degli utenti distribuito su blockchain Ethereum

lo stato attuale dei servizi di IM














































altri servizi "sicuri al 100%" usati dai terroristi:





where to begin...



	PRICE	AVAILABLE ON	TEXT CHAT	VIDEO CALLS	AUDIO CHAT	STICKERS	GAMES	WEB APP
 BBM	FREE							
 CHATON	FREE	   						
 CUBIE	FREE	 						
 FACEBOOK	FREE	   						
 GROUPME	FREE	  						
 HANGOUTS	FREE	 						
 HIKE	FREE	   						



# i problemi dei servizi centralizzati

anche nei servizi più sicuri come Signal

- Fuori dal nostro controllo
- Facilmente bloccabili / censurabili
- Single point of failure [tecnico / amministrativo / politico]
- La community non potrà mai essere davvero parte del progetto
- Limitati dalle scelte di sviluppo di altri
- Non modulari / estensibili

# cable: rete signal federata

un progetto di torn [autistici.org]



- Nasceva dall'idea di "ri"-decentralizzare Signal usando del vecchio codice usato in origine dal servizio.
- Di difficile manutenzione nel tempo viste le due strade divergenti fra il team OWS e il team Cable.
- Presentato a Hackmeeting 2017 in Val Susa.
- Gio [eigenlab Pisa / LibreMesh] espone ulteriori idee a riguardo e ravviva il ricordo di XMPP.



# XMPP

un vecchio amico



- Palinuro e MiBoFra di FrozenBox / Parrotsec infondono ulteriore ispirazione sul mondo XMPP.
- Diventa chiaro che è lo standard perfetto per questo scopo.
- Nel settembre 2017 inizia lo sviluppo di [aenigma](#).

# Il ritorno alla luce di XMPP

“Extensible Messaging and Presence Protocol”



“Extensible Messaging and Presence Protocol (XMPP) (precedentemente noto come Jabber) è un insieme di protocolli aperti di messaggistica istantanea e presenza basato su XML. Il software basato su XMPP è diffuso su migliaia di server disseminati su Internet; secondo la XMPP Standards Foundation (precedentemente nota come Jabber Software Foundation), già nel 2003 era usato da circa dieci milioni di persone in tutto il mondo.”

– [wikipedia](#)

# Conversations e OMEMO

Daniel Gultsch e il port di signal protocol nel mondo XMPP



- Si rende conto di come lo stato di XMPP fosse scandalosamente datato e non di fatto utilizzabile.
- Scrive Conversations [il primo vero client XMPP moderno] per Android.
- Porta signal protocol nel mondo XMPP con OMEMO [Omemo MultiEnd Message and Object crypto].

# XEP-0387 e la standardizzazione

## XMPP offre finalmente un protocollo universale

Current session established	just now
XEP-0163: PEP (Avatars / OMEMO)	available
XEP-0191: Blocking Command	available
XEP-0198: Stream Management	available
XEP-0237: Roster Versioning	available
XEP-0280: Message Carbons	available
XEP-0313: MAM	available
XEP-0352: Client State Indication	available
XEP-0363: HTTP File Upload	available
6d93b26b 35a2d2c3 2ac5c8fc 7e8b9bd2 08665c44 e0716afe 239a76b6 bf1a8b00	
Own OMEMO fingerprint	

- Ogni modulo di XMPP è definito da una XEP.
- La meta-XEP-0387 definisce i criteri di compatibilità che ogni client/server moderno deve supportare.
- <https://xmpp.org/extensions/xep-0387.html>

# i server XMPP ed ejabberd

## la prima implementazione di ejabberd in aenigma



- L'istanziamento di ejabberd si rivela estremamente complessa e la documentazione piena di lacune.
- Serviva un sysadmin
- Io \*odio\* i sysadmin [e lo faccio anch'io per lavoro, almeno ci provo, per finta, di solito...]

rage against the sysadmins

vogliamo loro bene, ma sono un disastro [spesso e volentieri]



- accrocchi custom made tramite trial and error e stackoverflow non sono il futuro della tecnologia.
- quando qualcuno si accorge che il loro lavoro non funziona sono già in pensione.
- sono tanti ma [per fortuna] non sono tutti come loro.

# i sistemi di automazione

## un'ancora di salvezza in un oceano di delirio



- ambiscono a fare il lavoro una volta sola, farlo nel migliore dei modi, scriverlo, e dividerlo.
- creano uno standard di eccellenza procedurale accessibile a tutti.
- focalizzano il lavoro degli altri sui miglioramenti e non sulle repliche di risultati già ottenuti.

# falsi miti dell'automazione

["ci rubano il lavoro!" -cit]

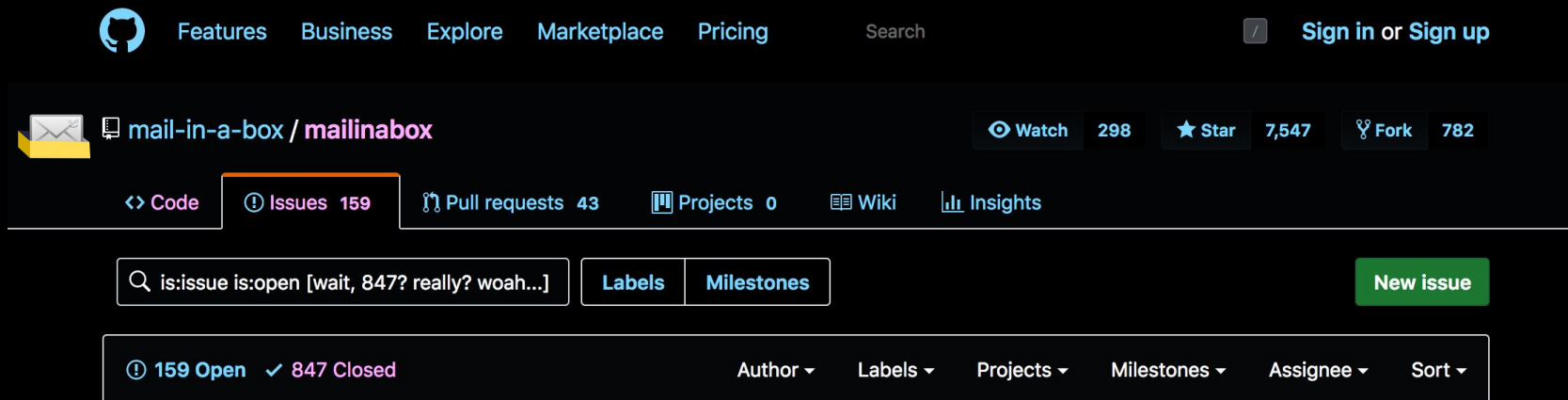


- "abbiamo tutti bisogno di soluzioni custom designed e custom made"
- "le macchine sbagliano, e loro nemmeno se ne rendono conto"
- "sta installando tutti i pacchetti della repo universe!!!"
- "se la terra davvero non è piatta allora spiegatemi come funzionano le ruote dei criceti in australia!"



# mail-in-a-box

## il mail server self-hosted per tutti



The screenshot shows the GitHub repository page for mail-in-a-box/mailinabox. The repository has 298 watches, 7,547 stars, and 782 forks. The 'Issues' tab is selected, showing 159 open issues. The search bar contains the text 'is:issue is:open [wait, 847? really? woah...]'. The repository name is 'mail-in-a-box / mailinabox'.

Features Business Explore Marketplace Pricing Search Sign in or Sign up

mail-in-a-box / mailinabox

Watch 298 Star 7,547 Fork 782

Code Issues 159 Pull requests 43 Projects 0 Wiki Insights

is:issue is:open [wait, 847? really? woah...] Labels Milestones New issue

159 Open 847 Closed Author Labels Projects Milestones Assignee Sort

- sedicentimiliardi di bug affrontati e fixati.
- alcuni dei quali incredibilmente proprio relativi all'enorme difficoltà di tirare su un mxserver fatto bene
- nessuno di voi fino ad ora sapeva che il TTL dei record NS richiesti dal NIC .IS è di 86400". [gotcha]

# streisand

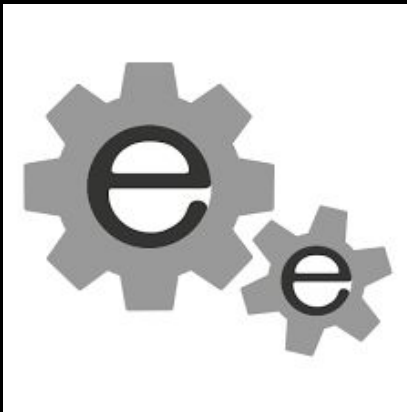
il vpn server self-hosted per tutti



- risultati concreti come un progetto della nasa ma con un budget ancora minore [e ho detto tutto]
- lo sviluppatore stesso ammette che nessuno sarebbe in grado di farlo da solo [told you so]
- hmmm aspetta com'è possibile che la config di wireguard stia tutta dentro 20 righe di codice?

# easyengine

il server nginx + wordpress + docker self-hosted per tutti



- ottengono un A+ su ssltest ad ogni sito creato e non scrivono neanche un blogpost dal titolo clickbait!
- guarda la cronologia del browser: quante volte hai fatto copia-incolla da cipherli.st?
- non mi dire, ogni sito ha un container che lo isola dagli altri siti! ma non sarà troppa sicurezza adesso?

# synthia + dna

aenigma diventa un framework bash + git



- ogni progetto è istanziabile con un git clone, tre righe di codice cambiate, ed una git push.
- tutte le funzioni sono standardizzate dentro una repo unica sourceata ad ogni esecuzione.
- chi diavolo è synthia???

# raptor: automazione recursiva

## wait what?



- lavora ad un livello sopra easyengine
- aggiunge funzionalità di backup / restore criptato remoto automatico notturno su S3 e accesso SFTP
- basato su synthia+dna

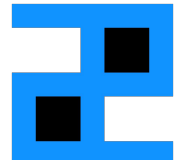
functions	README.md	aenigma-cluste...	aenigma-exec	aenigma-push_...	aenigma-creat...	setup	aenigma-env	aenigma-test-o...	aenigma-upgra...
-----------	-----------	-------------------	--------------	------------------	------------------	-------	-------------	-------------------	------------------

```

1  #!/usr/bin/env bash
2
3  ### openspace synthia bootstrap framework
4  ### [https://github.com/openspace42/synthia]
5  ### v0.3.1
6
7  os_dna_version="v0.3.2"
8
9  #####
10
11 synthia_define_vars() {
12
13     #####
14     ##### Insert your initial variables here #####
15     #####
16
17     export proj_name="aenigma"
18     export author_name="openspace42"
19     export git_host="https://github.com"
20
21     ### Set this to `y` if your project stores no data on end users' machines that could go lost during a re-install
22     export skip_install_time_backup="n"
23
24     ### Set this to the directory that has the most impactful size when performing a backup [such as `/var/www/` for
25     export backup_ref_dir="/var/lib/ejabberd"
26
27     #####
28     #####
29     #####
30
31     ### Do NOT edit the following line
32
33     dna_define_vars
34
35     #####
36     ##### Insert your additional variables here #####

```

aenigma  
demo time





Nicolas North | [nz@os.vu](mailto:nz@os.vu)

<https://openspace.xxx>