



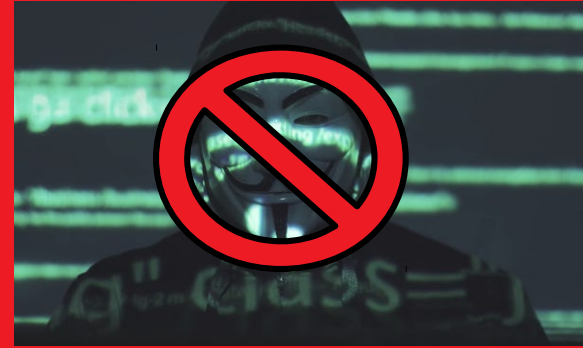
Becoming Anonymous

Part III - Infrastructure

@bugg



DISCLAIMER!!!



- This is not legal advice!
- This is a **FANTASY BACKDROP** for learning about Cybersecurity
- This has not been done IRL
- If you do this IRL you are committing a **CRIME!**



Series Overview

- Part I – Overview
- Part II – Intel
- Part III – Infrastructure
- Part IV – Recruiting
- Part V – Action



Infrastructure Overview

- Real-Time Communication
- Information Storage Platform
- Several Needs
- Many Wants



Wants and Needs

- Needs
 - Secure
 - Anonymous
- Wants
 - Easy
 - Robust
 - Decentralized
 - Ephemeral



Challenges

- Hosting
- Payments
- Software Changes
- Maintainability
- Migrations



Real-Time Communication

- Vetting Process
- Daily Communications?
- Meetings
- Group/Shared Task Communications
- Builds rapport



Real-Time Communication

- IRC running as a Hidden Service on a VPS
- IRC
 - BBS → Twitch Chat (yes really)
 - ngIRCd → simple, easy, effective
- Hidden Service
 - Tor/TOR/T.O.R. → forced anonymity for server and clients
- VPS
 - Ubuntu Server Latest → simple, easy, reasonably secure
 - Fast/Cheap to spin up new nodes



Information Storage Plat.

- Data, Information, Intelligence needs a home
- Long-term storage (non-ephemeral data)
- Group policies
- Group layout
- Infrastructure information (addresses)



Information Storage Plat.

- Apache hosted HTML (Wiki) as Hidden Service synced with wget backed up with Borg on a VPS
- HTML
 - Easy, Simple, Secure (no JS BS)
 - Apache → Literally no config
- Hidden Service
 - Tor/TOR/T.O.R. → forced anonymity for server and clients
- Syncing
 - To keep the nodes in sync
 - wget → extremely robust and straightforward
- Backups
 - To recover from bad updates
 - Borg → easy and de-duplicating
- VPS
 - Ubuntu Server Latest → simple, easy, reasonably secure
 - Fast/Cheap to spin up new nodes



Layout - IRC

- Two distinct IRC networks
 - IRC networks are composed of nodes
- IRC Nodes are decentralized
- More node-runners = More redundancy
 - Decentralization doesn't benefit from single-user redundancy
- First network
 - Introductory point for vetting
 - Should vetting be approved new member gets link to Second network
- Second network
 - Where the actual comms happen

Layout - Wiki

- Wiki nodes are decentralized
- More node-runners = More redundancy
 - Decentralization doesn't benefit from single-user redundancy
- Node-runners
 - Know how to manage their node
 - Make it easy to get right
 - Make it hard to get wrong
- Bad actors get purged then everybody rolls back
- Updates from non-node-runners are manual (not as easy)

The DATDA Collective (TDC)

