



Becoming Anonymous

Part II - Intel

@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

Intel Overview

- Data → Information → Intelligence
- Intelligence has significance and relevance
- Working towards
 - Exploitative Intelligence
 - De-Anonymization Intelligence

Intelligence?

- Gathering Intelligence
 - Ex: Gather Data about a site
- Exploiting Intelligence
 - Ex: Use a SQL Injection found by a scan
- Disseminating Intelligence
 - Ex: Handover real IP of server to FBI

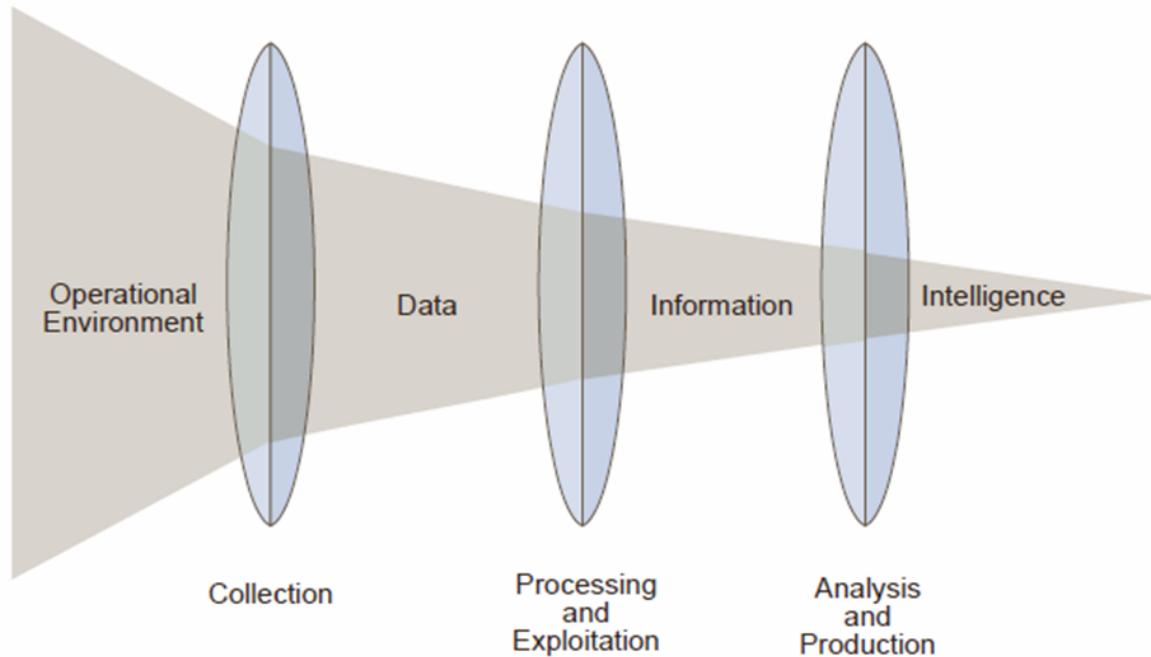


Intelligence

- Data is collected and processed into Information
 - Ex: A database of usernames and passwords
- Information is analyzed to determine Intelligence
 - Ex: The usernames and passwords in the database
- Intelligence has significance and relevance
 - Ex: The username and password of a targeted user

Intelligence

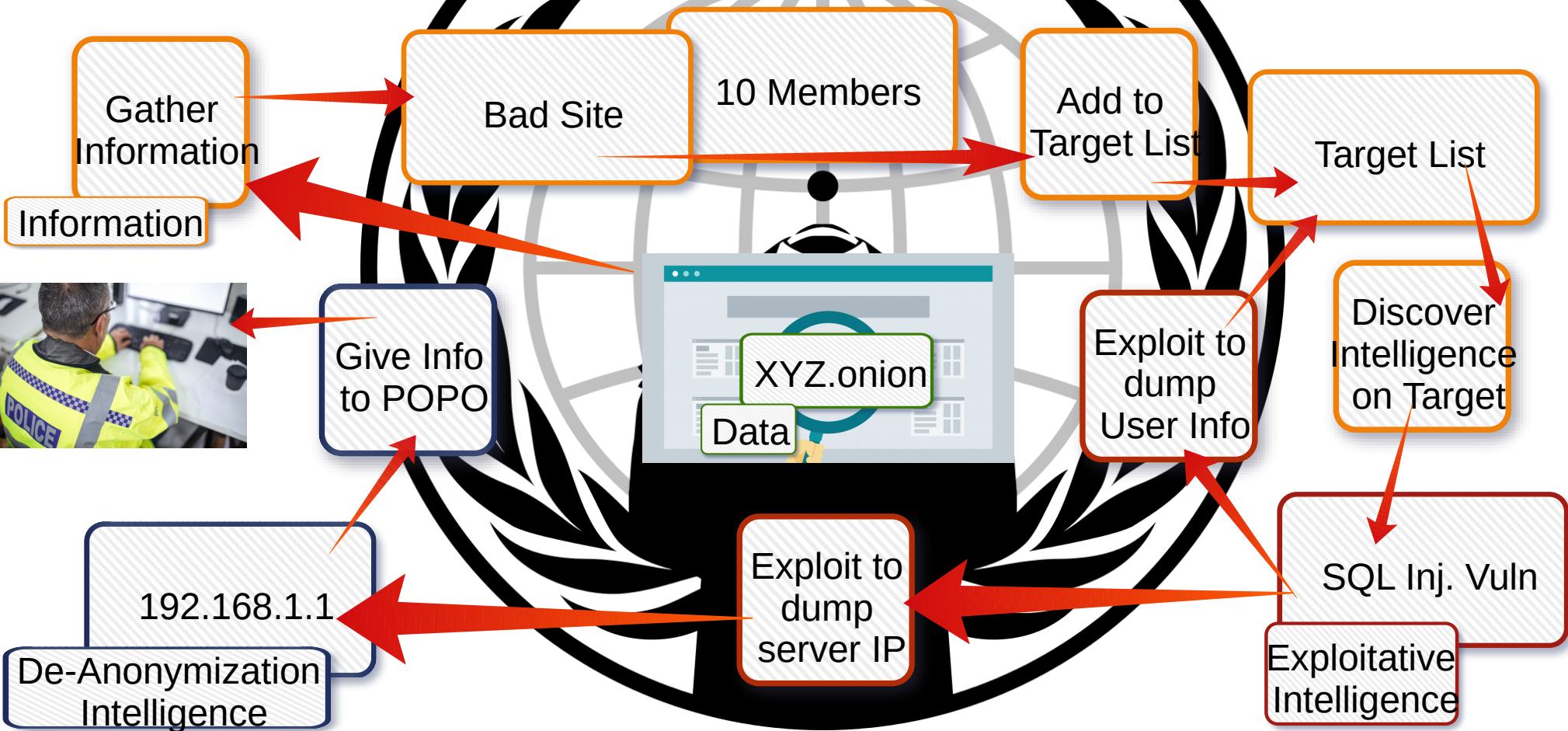
Relationship of Data, Information and Intelligence



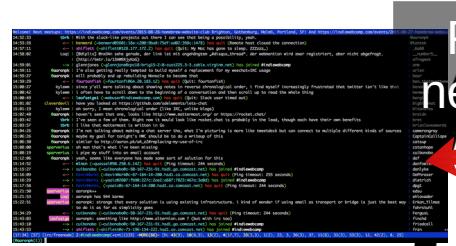
Two types of Intelligence

- Exploitative (Action) Intelligence
 - Can be exploited for our gain
 - Generally exploited through action
- De-Anonymization Intelligence
 - Can de-anonymize (dox) an individual/system/etc.
 - Generally given to Law Enforcement

Our Intelligence Cycle



The DATDA Collective (TDC)



Posts
new link



Puts link
in Target
List



Starts
Targeting
Site



Finds
Address

inf_id	number	Address
1	1	355 Miller Stargell Ave., Alameda, CA 94501
2	2	1210 N. Alberic Blvd., Alameda, CA 94501
3	3	190 E. Stacy Rd., Alton, TX 75002
4	4	401 S. Main St., American Fork, UT 84003
5	5	1568 State College Blvd., Anaheim, CA 92806
6	6	600 S. Brookhurst, Anaheim, CA 92804
7	7	5646 E. La Palma, Anaheim, CA 92807
8	8	1230 W. 1st St., Arcadia, CA 91006
9	9	1075 W. I-20, Arlington, TX 76017
10	10	1170 W. Brand St., Arroyo Grande, CA 93420

Sends
Address to
POPO



Arrests
Site
Operator

