



UNIVERSITY OF PADUA
UNIVERSITA' DEGLI STUDI DI PADOVA



SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

Boten ELISA

*A Novel Approach for Botnet C&C
in Online Social Networks*

IEEE Conference on Communications and Network Security (CNS),
Florence - September 28th, 2015

Alberto Compagno*, Mauro Conti , Daniele Lain , Giulio Lovisotto , Luigi Vincenzo Mancini*

* Department of Computer Science
Sapienza University of Rome, Italy

 Department of Mathematics
University of Padua, Italy

Botnet Introduction

- *Overview*
- *Evolution*

ELISA - a Novel Botnet Proposal

- *Structure*
- *C&C channel*
- *Examples*
- *Evaluation*

Conclusions and Future Work

Bots - *Machines compromised by a malware*

Botmaster - *Entity controlling the bots (attacker)*

C&C - *Channel used for the botnet communications*

One of the **most serious threats** against cyber-security:

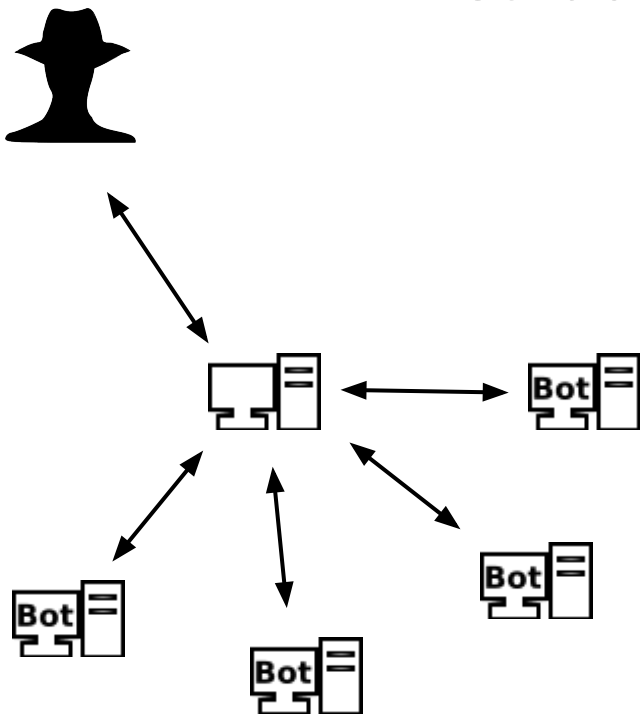
- *Difficult to detect*
- *Hard to prevent*
- *Can be huge*

BBC NEWS | 1 June 2015
Hola rocked by botnet accusations

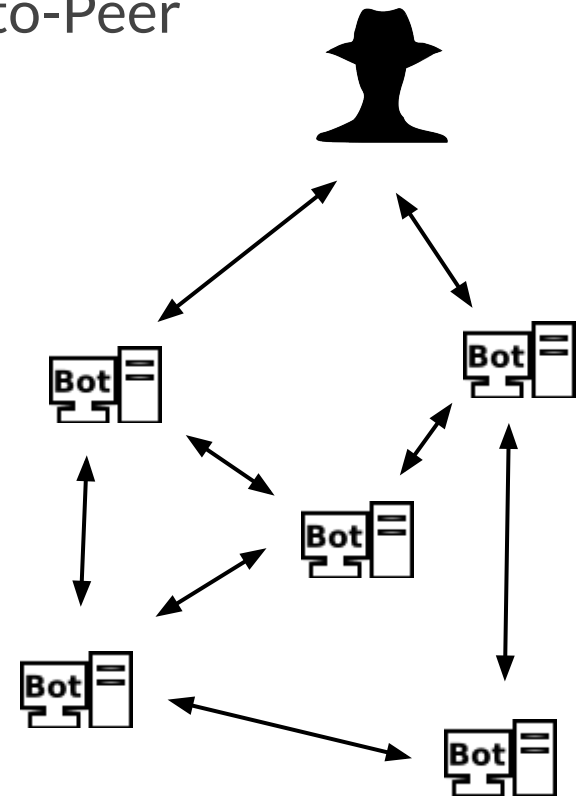
The New York Times | JAN. 22, 2009
Worm Infects Millions of Computers Worldwide

WIRED.CO.UK | MALWARE / 25 FEBRUARY 15
Europol cracks down on botnet infecting 3.2m computers

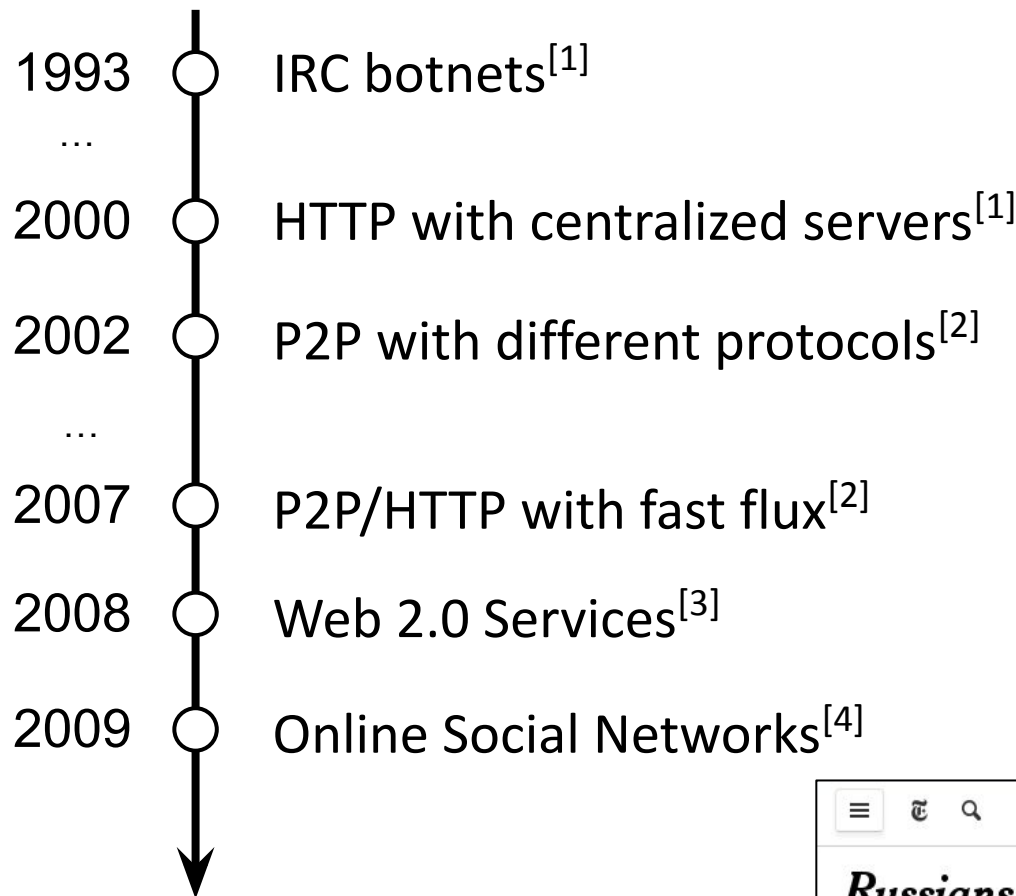
Centralized



Peer-to-Peer



Evolution of botnet C&C



[1] - *An Inside Look at Botnets*, Barford (2007)

[2] - *An Analysis of the Asprox Botnet*, Borgaonkar (2010)

[3] - *Botnet with Browser Extensions*, Liu (2011)

[4] - *The Koobface Botnet and the Rise of Social Malware*, Thomas (2010)

Active: modify potential C&C packets, observe reactions

Passive: observe the network traffic to find:

- *patterns (by correlations and behaviour)*
- *clusters of similar nodes*

A hot research topic with many contributions

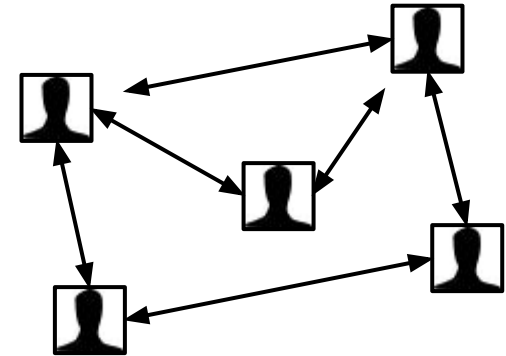
(*BotTrack, BotyAcc, BotHunter, BotMiner, Disclosure, etc.*)

Goal

**Build a C&C channel that avoids detection
from network observers**

Online Social Network (*OSN*) as a graph

- **Nodes** are the users
- **Edges** indicate relationships
(such as friendship)



Malware can intercept and modify the information exchanged between users (victims) and the OSN

Botmaster has access to one or more OSN accounts

ELusive Social Army (ELISA)

- *OSNs as a mean to spread C&C messages*

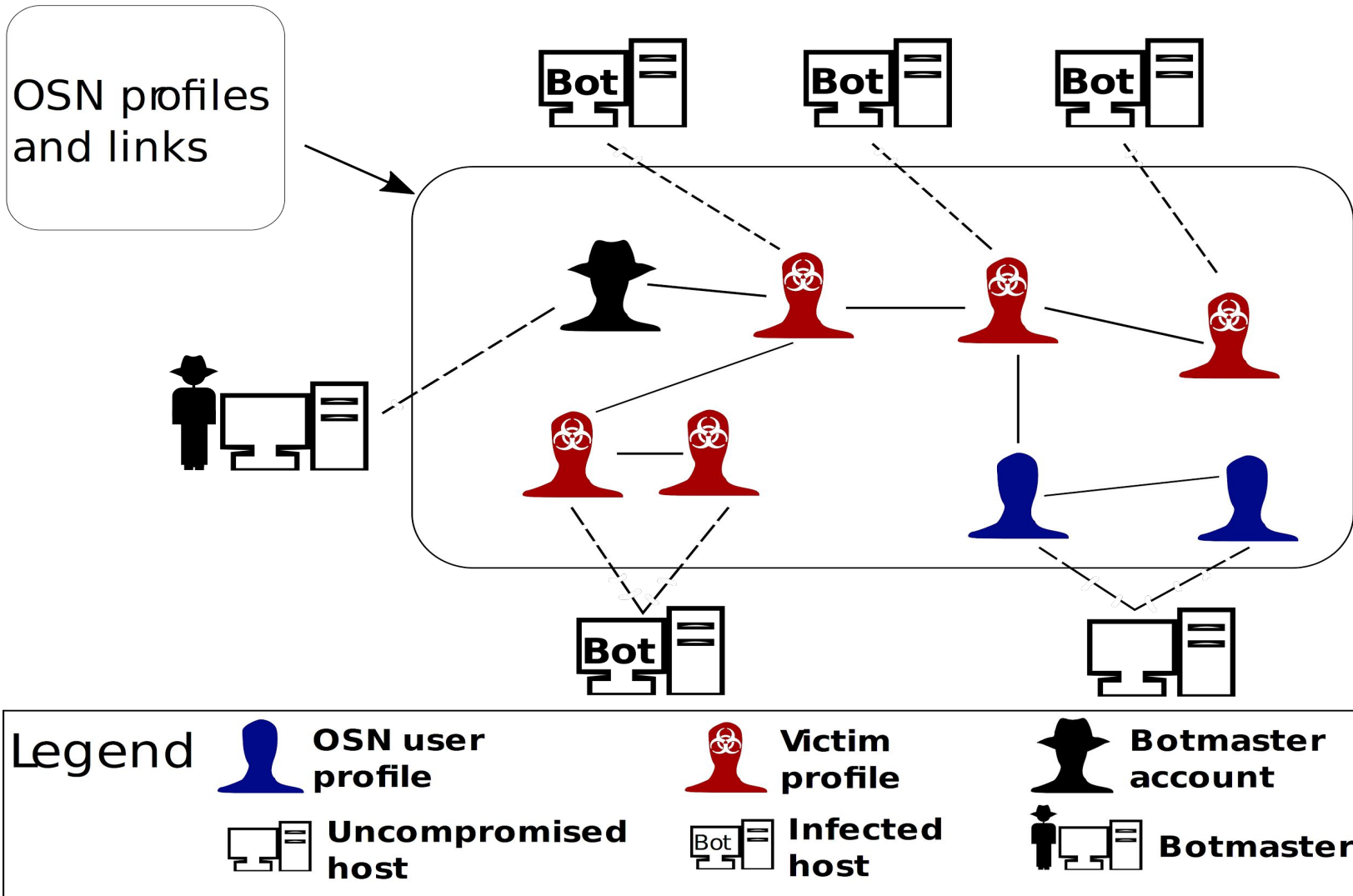
Unicode **steganography** to build a covert channel

- *Popular OSNs are “vulnerable” to this*

Opportunistic communication

- *Append C&C information to user generated content*

ELISA (Structure)



Characters with **invisible** glyph

(used, e.g., in internationalization)

- 11 on Facebook
- 23 on Google Plus

"Latin Small letter A"

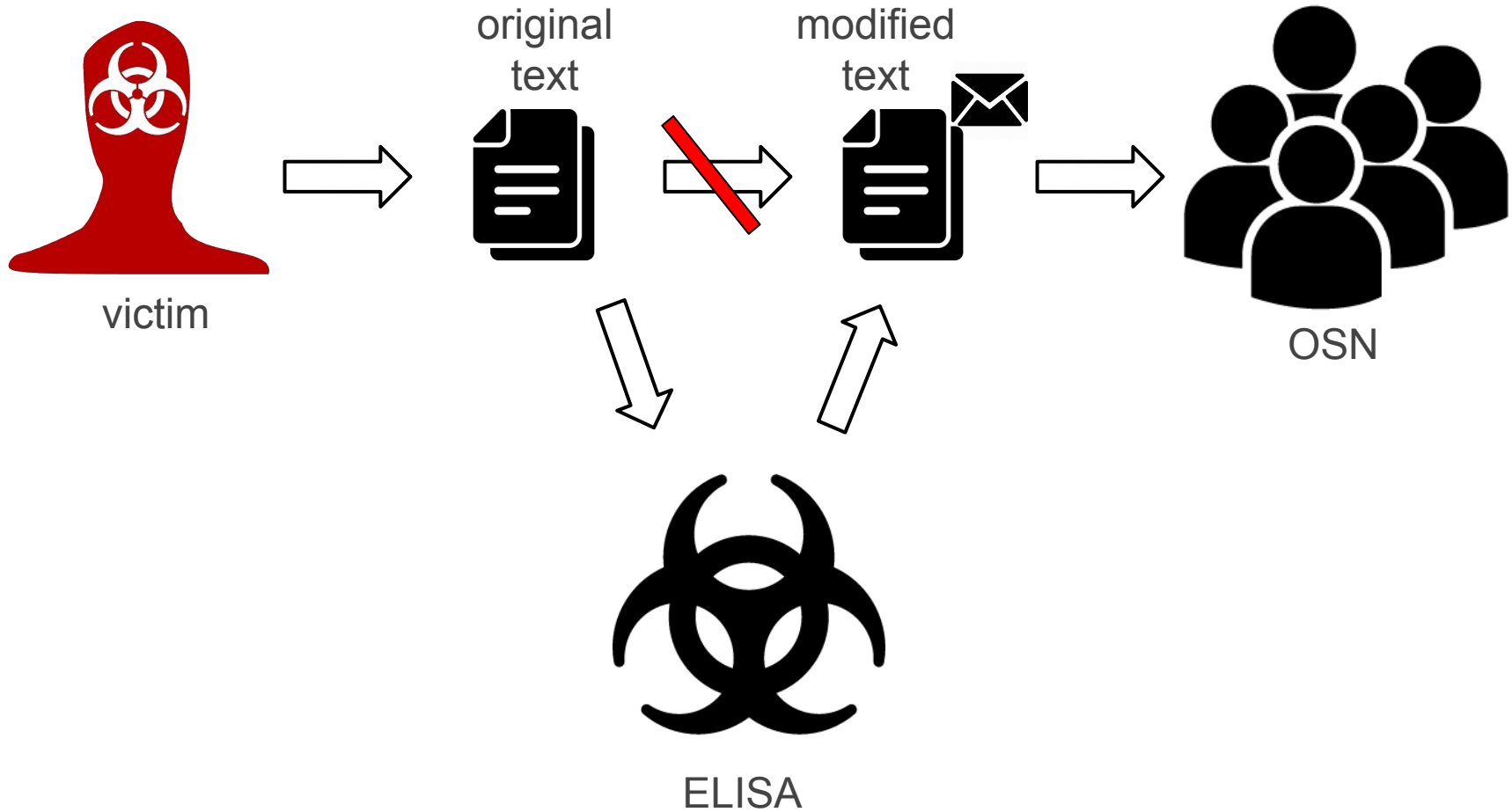
U+0061 → a

"Left-To-Right Mark"

U+200E →

N-ary Huffman algorithm → ELISA's alphabet

Function to map letters to non-printing characters, and vice-versa



Botmaster account



The screenshot shows a Facebook profile for a user named "Bot Master". The profile picture is a generic silhouette. The bio says "Modifica profilo". The navigation menu on the left includes "Benvenuto", "Notizie", "Messaggi", and "Eventi". The main content area shows a post creation interface with the text "Hi I'm new on Facebook || ATTACK 8.8.8.8 1408806582". The post creation options include "Stato", "Aggiungi foto/video", "Amici", and "Pubblica".

Victim account



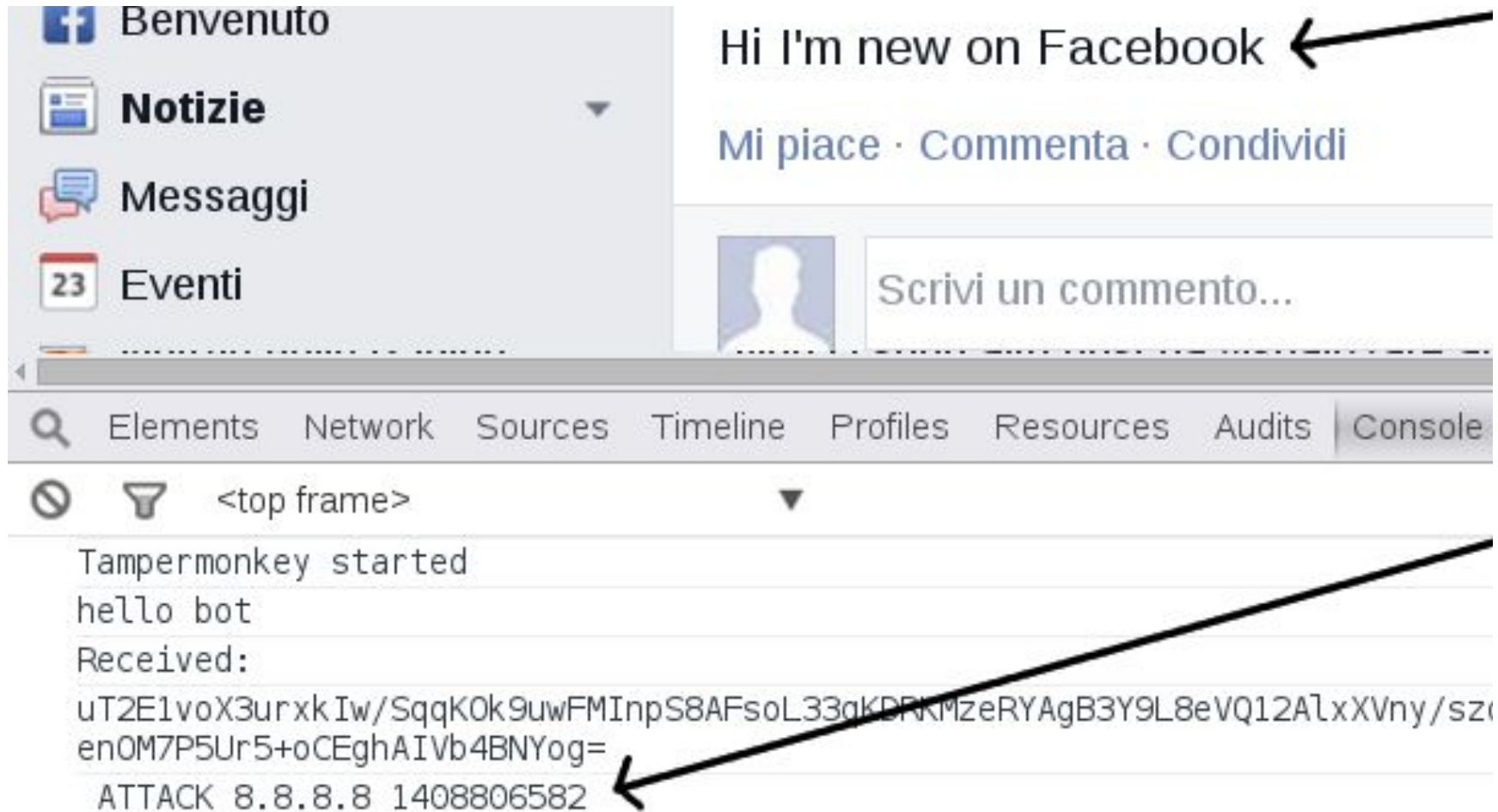
The image shows a screenshot of a Facebook profile for a user named "Poor Victim". The profile page displays a message from "Bot Master" that says "Hi I'm new on Facebook". A callout bubble points to this message with the text "message read by the user". Below the message is a comment input field with the placeholder text "Scrivi un commento...".

At the bottom of the screenshot, the browser's developer console is open, showing the following log entries:

```
Tampermonkey started  
hello bot  
Received:  
uT2E1voX3urxkIw/SqqKOk9uwFMInpS8AFsoL33qkDRkMzeRYAgB3Y9L8eVQ12A7xXVny/szow2tH9p8l88a8IEm+0m65sE1z1WaL0e0ua/7tNqCvamoU5srv2a/h  
enOM7P5Ur5+oCEghAIVb4BNYog=  
ATTACK 8.8.8.8 1408806582
```

A callout bubble points to the "ATTACK" log entry with the text "hidden message received by the bot".

Victim account



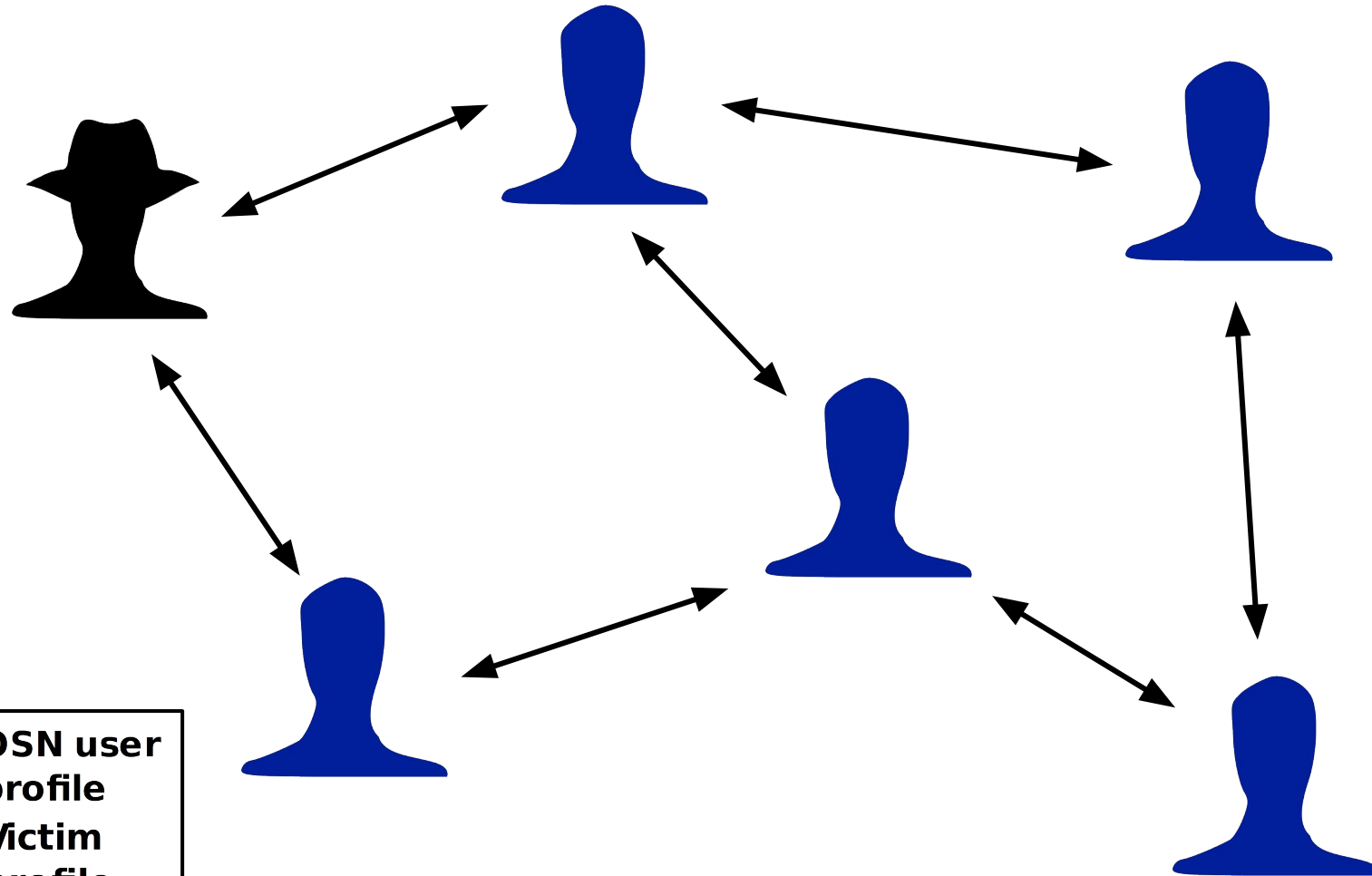
The image shows a screenshot of a Facebook post from a victim account. The post content is "Hi I'm new on Facebook" with interaction options "Mi piace · Commenta · Condividi". Below the post is a comment input field with the placeholder text "Scrivi un commento...".




Below the Facebook interface is a browser developer console. The console shows the following log entries:

```
Tampermonkey started  
hello bot  
Received:  
uT2E1voX3urxkIw/SqqK0k9uwFMInpS8AFsoL33gKDRKMzeRYAgB3Y9L8eVQ12A1xXVny/sz  
en0M7P5Ur5+oCEghAIVb4BNYog=  
ATTACK 8.8.8.8 1408806582
```

Two black arrows point to the post text and the final log entry in the console.

Propagation Example

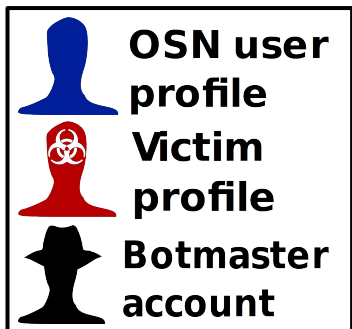
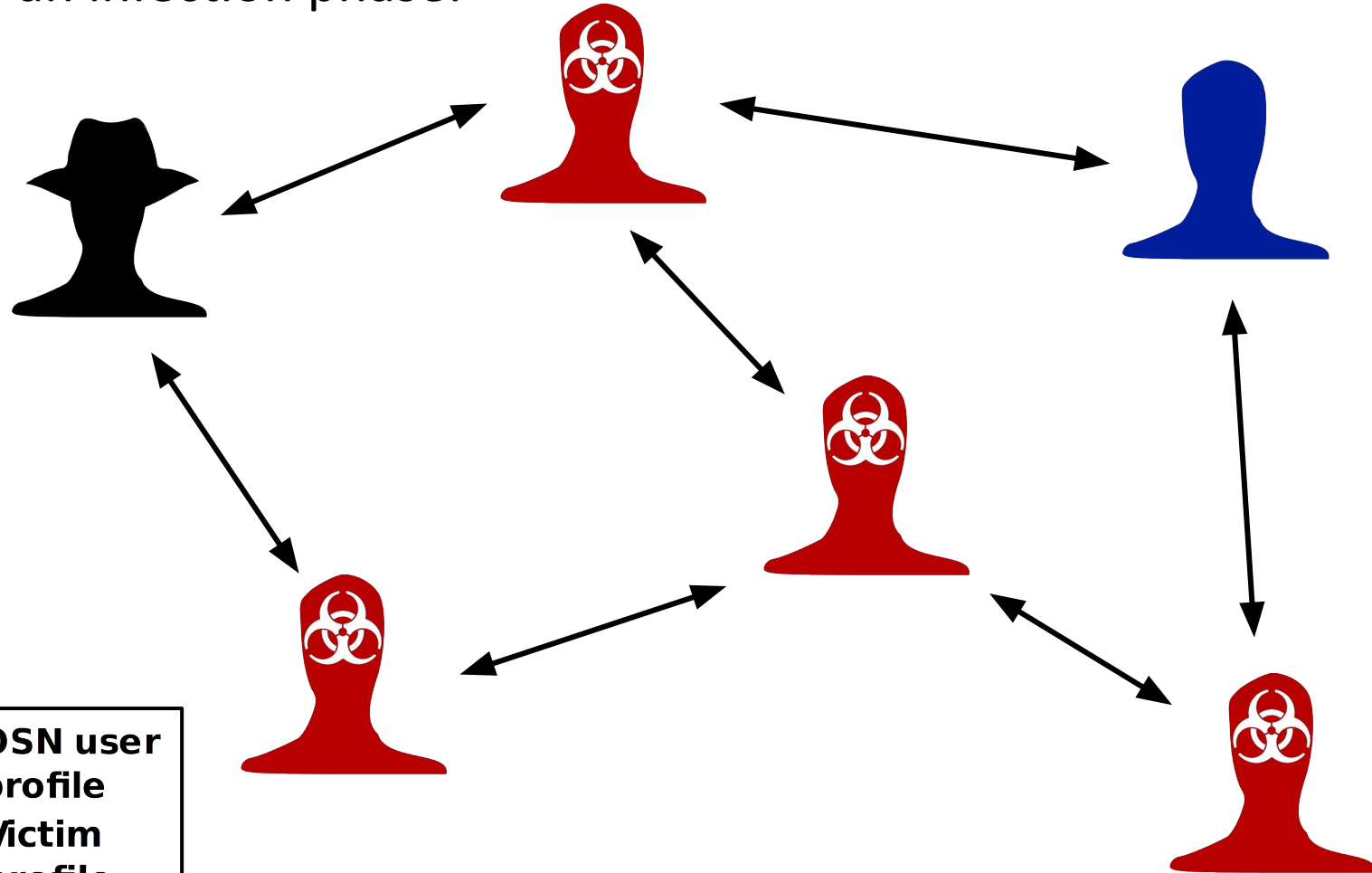


	OSN user profile
	Victim profile
	Botmaster account

Propagation Example



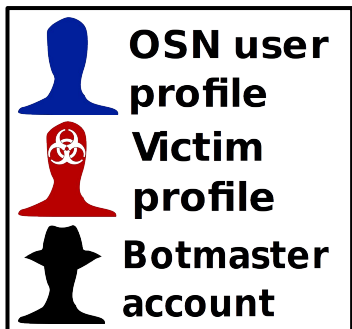
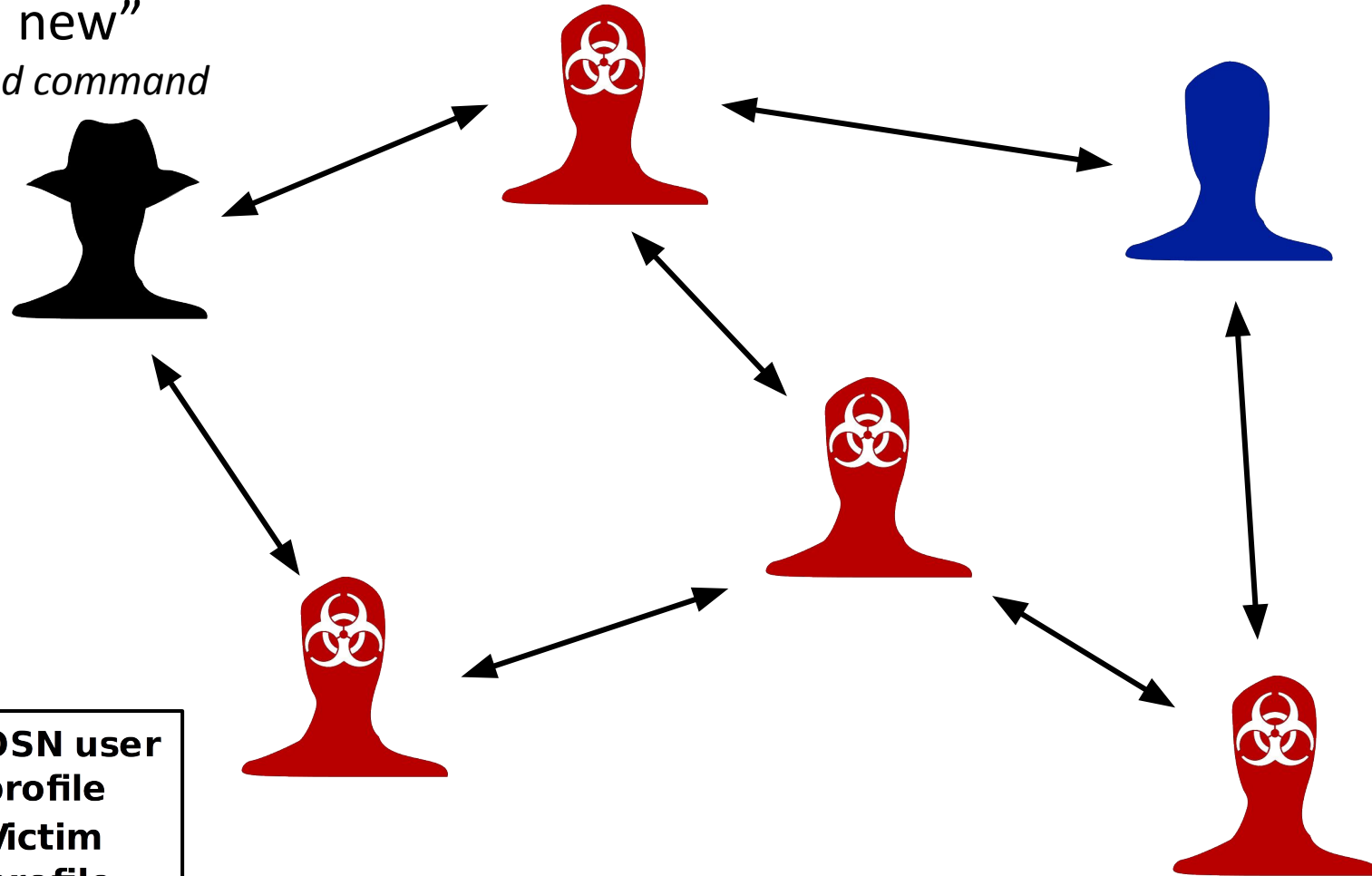
After an infection phase:



Propagation Example



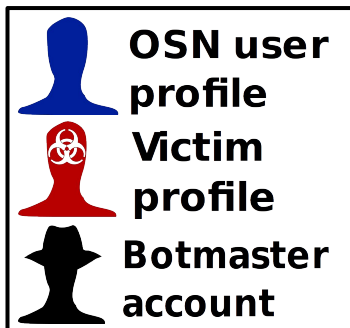
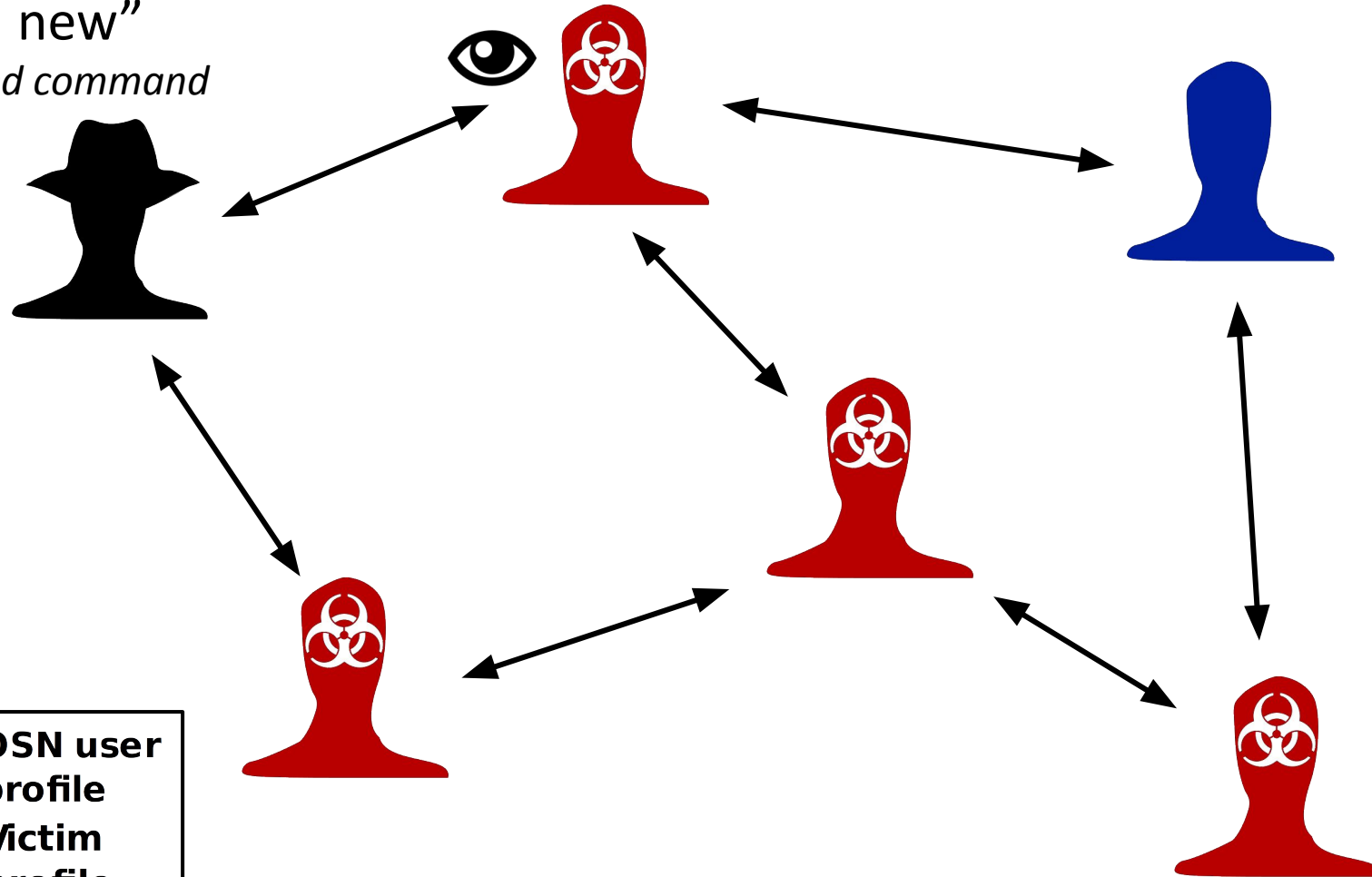
“Hi I’m new”
+ encoded command



Propagation Example



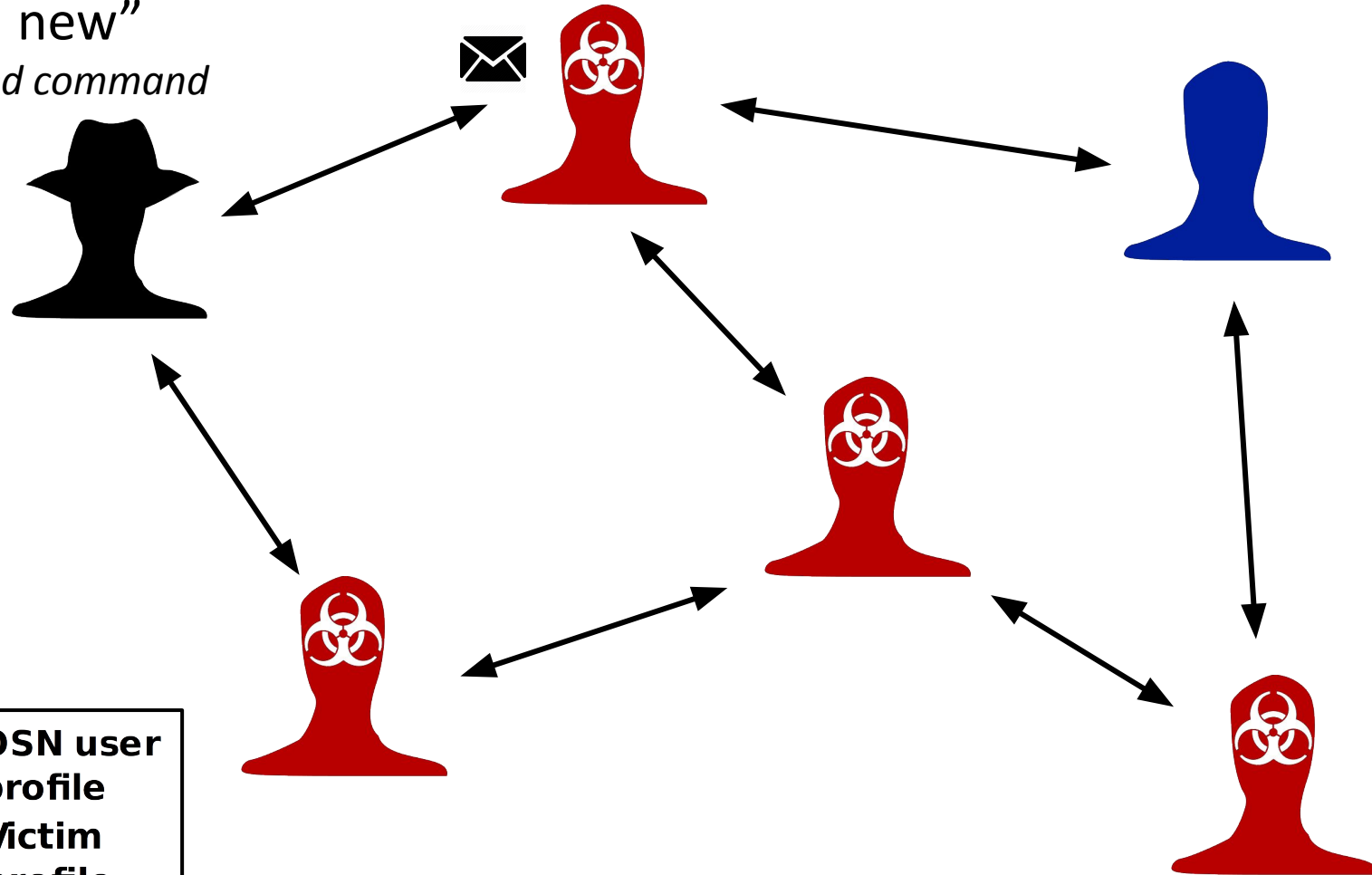
“Hi I’m new”
+ encoded command






Propagation Example



“Hi I’m new”
+ encoded command

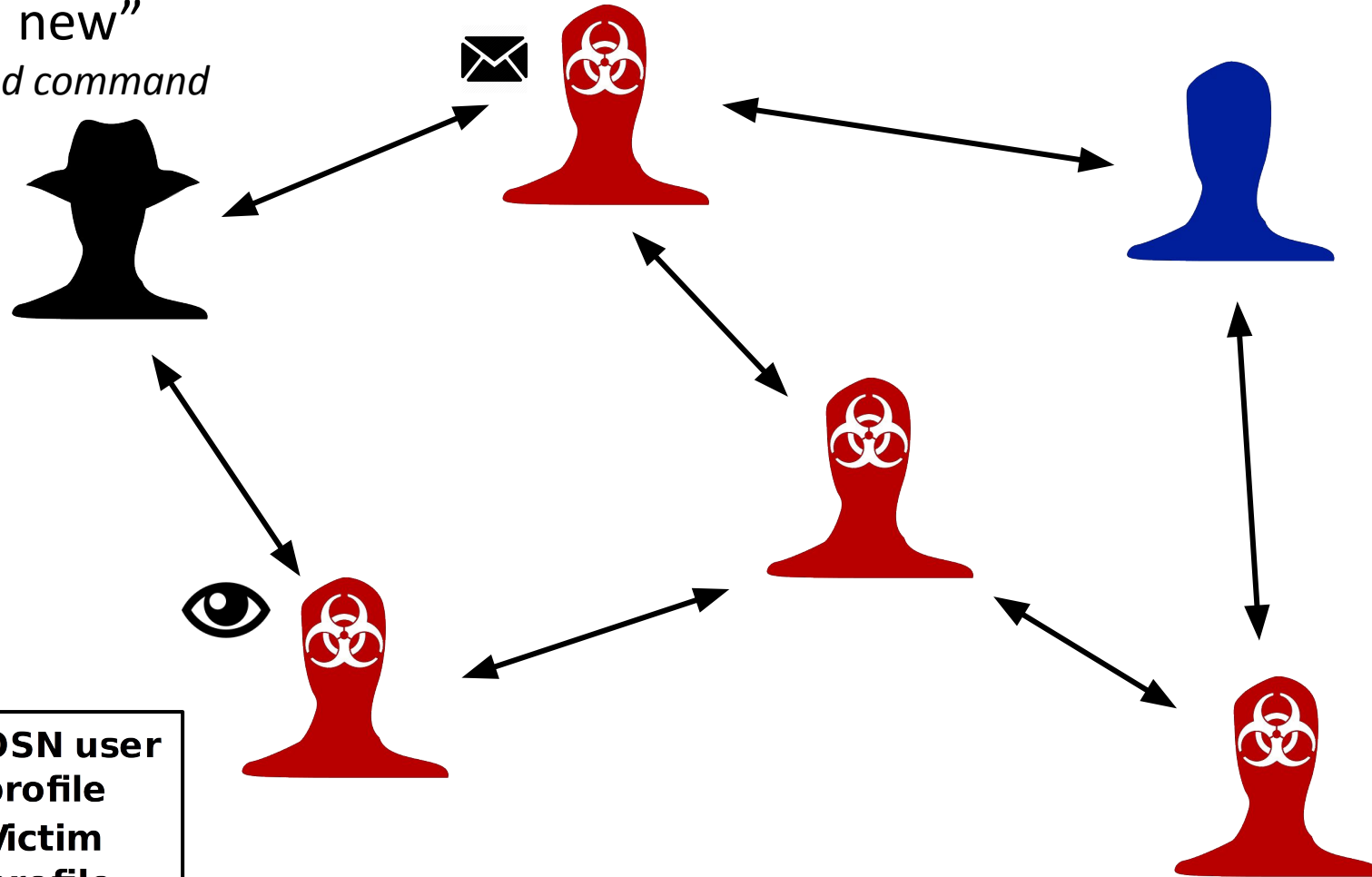





	OSN user profile
	Victim profile
	Botmaster account

Propagation Example

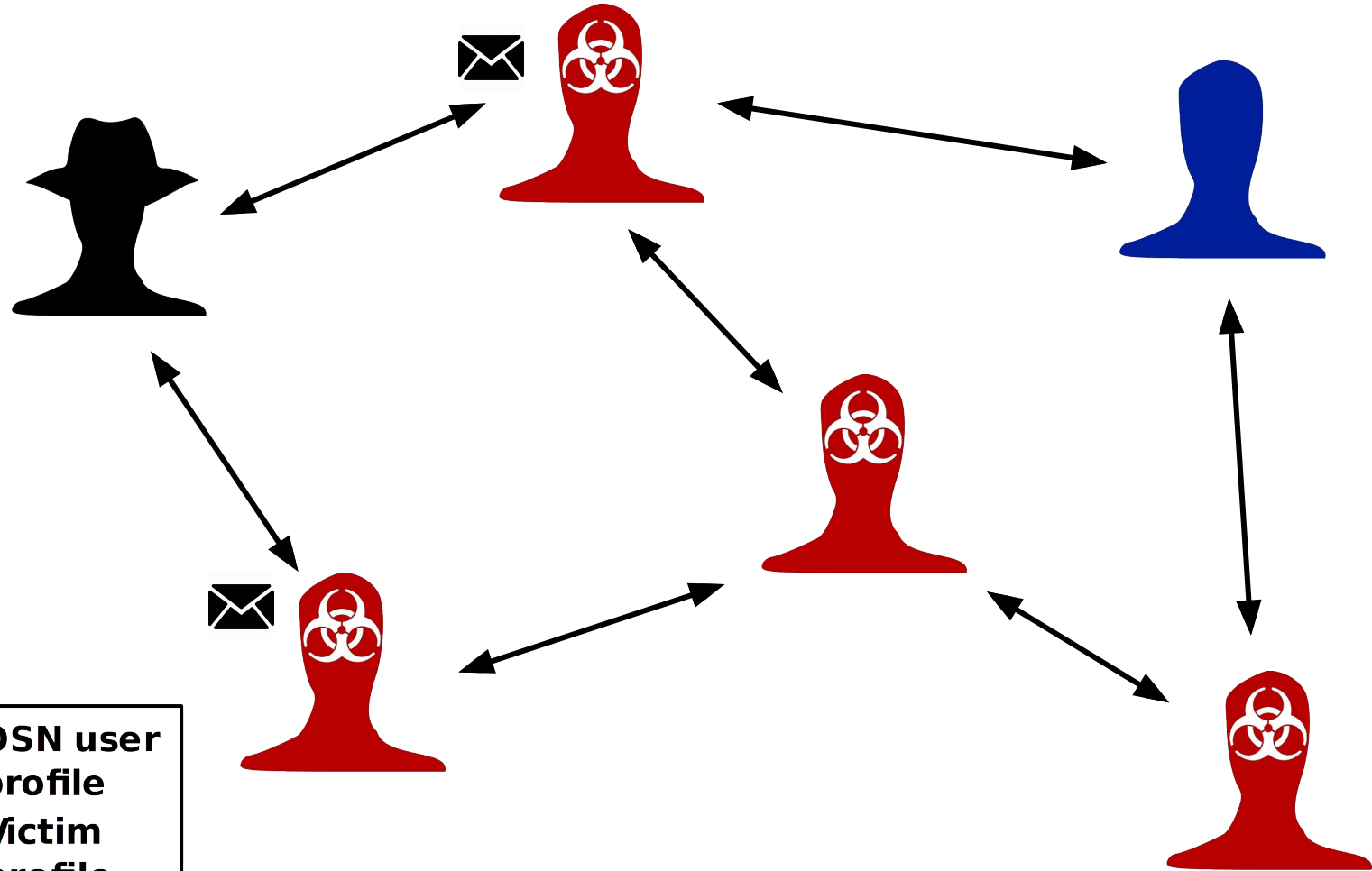





“Hi I’m new”
+ encoded command



	OSN user profile
	Victim profile
	Botmaster account

Propagation Example

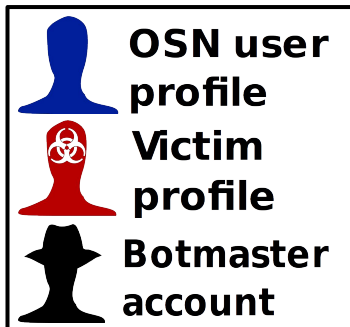
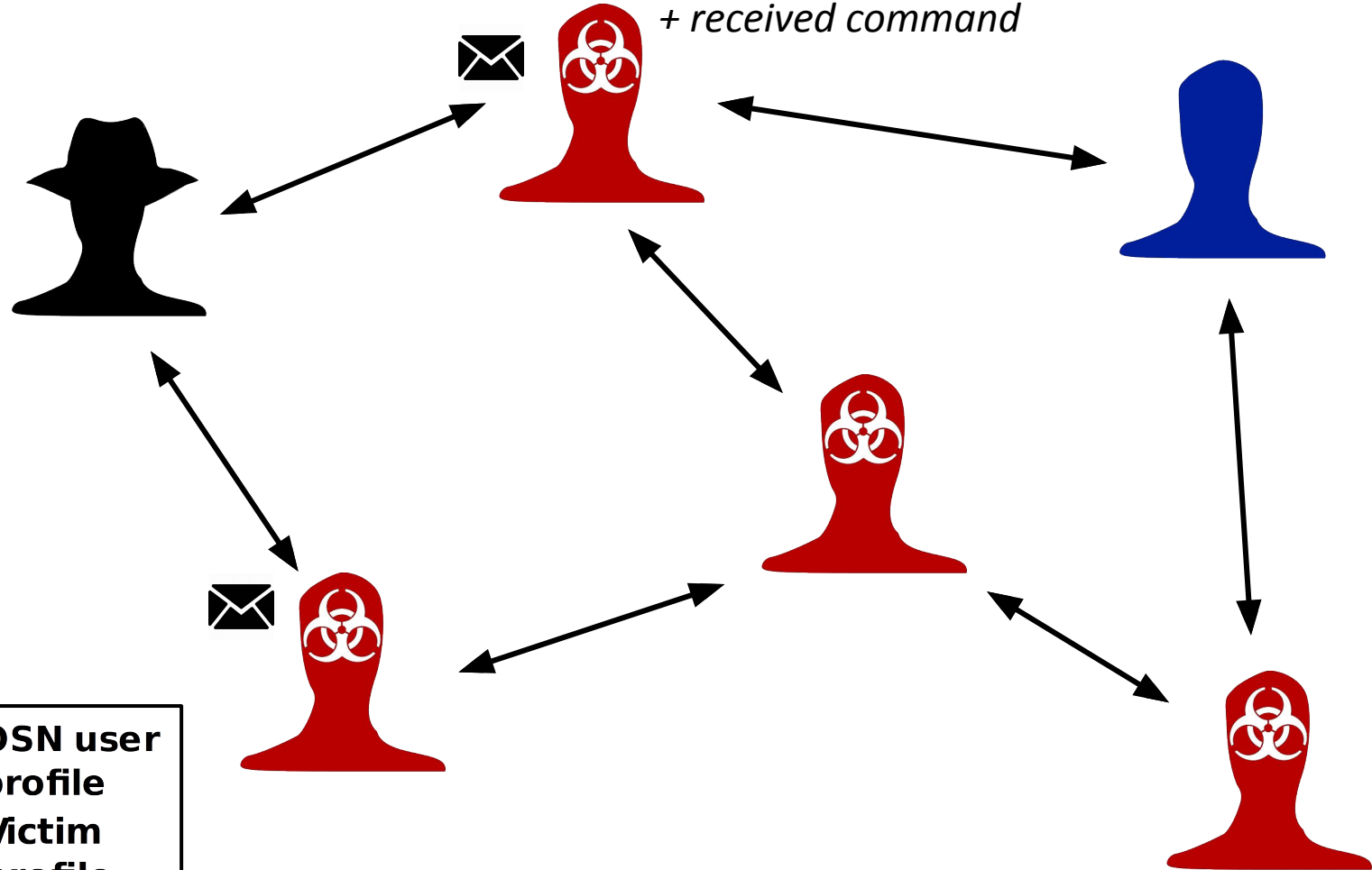


	OSN user profile
	Victim profile
	Botmaster account

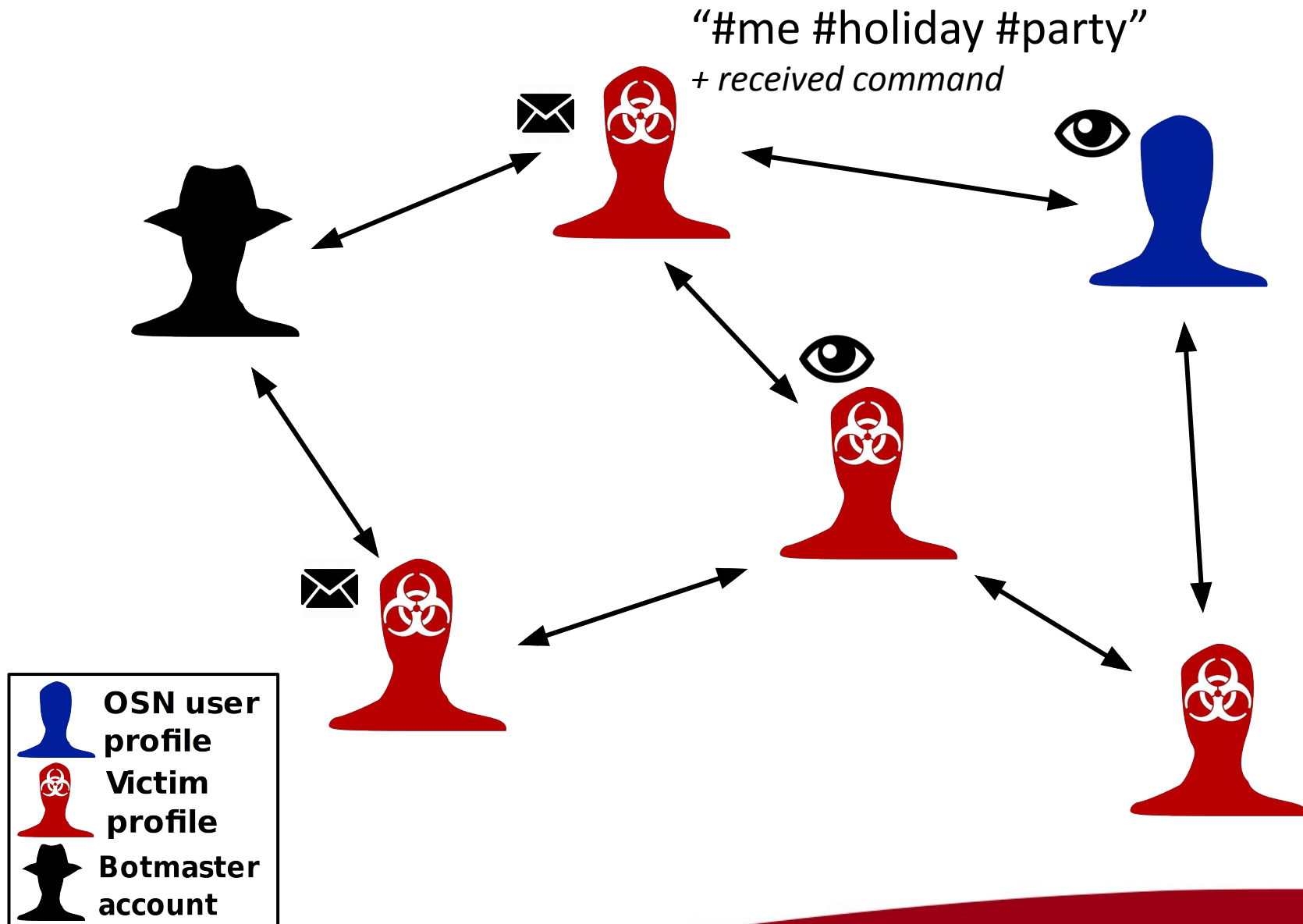
Propagation Example



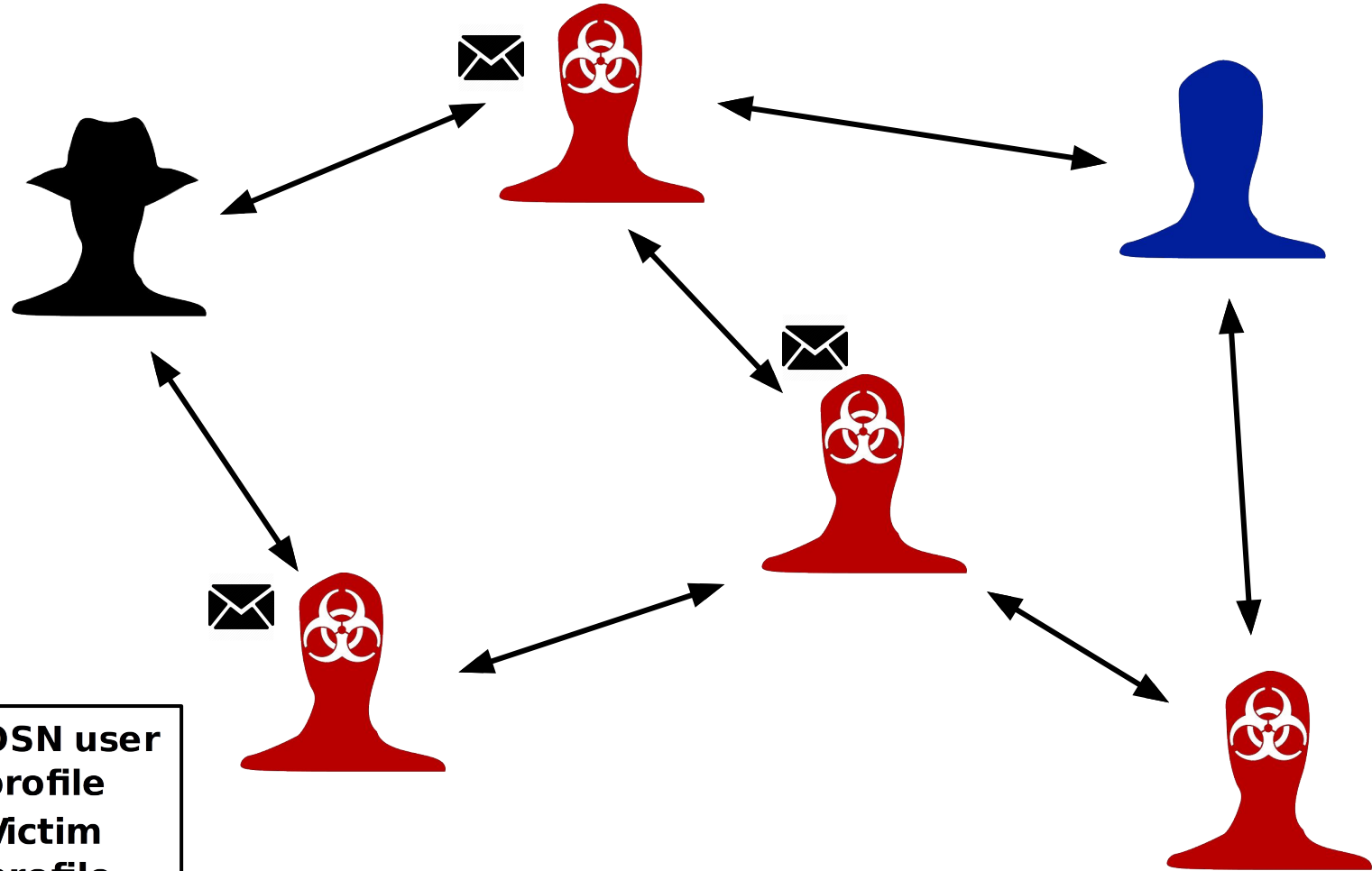
"#me #holiday #party"
+ received command






Propagation Example

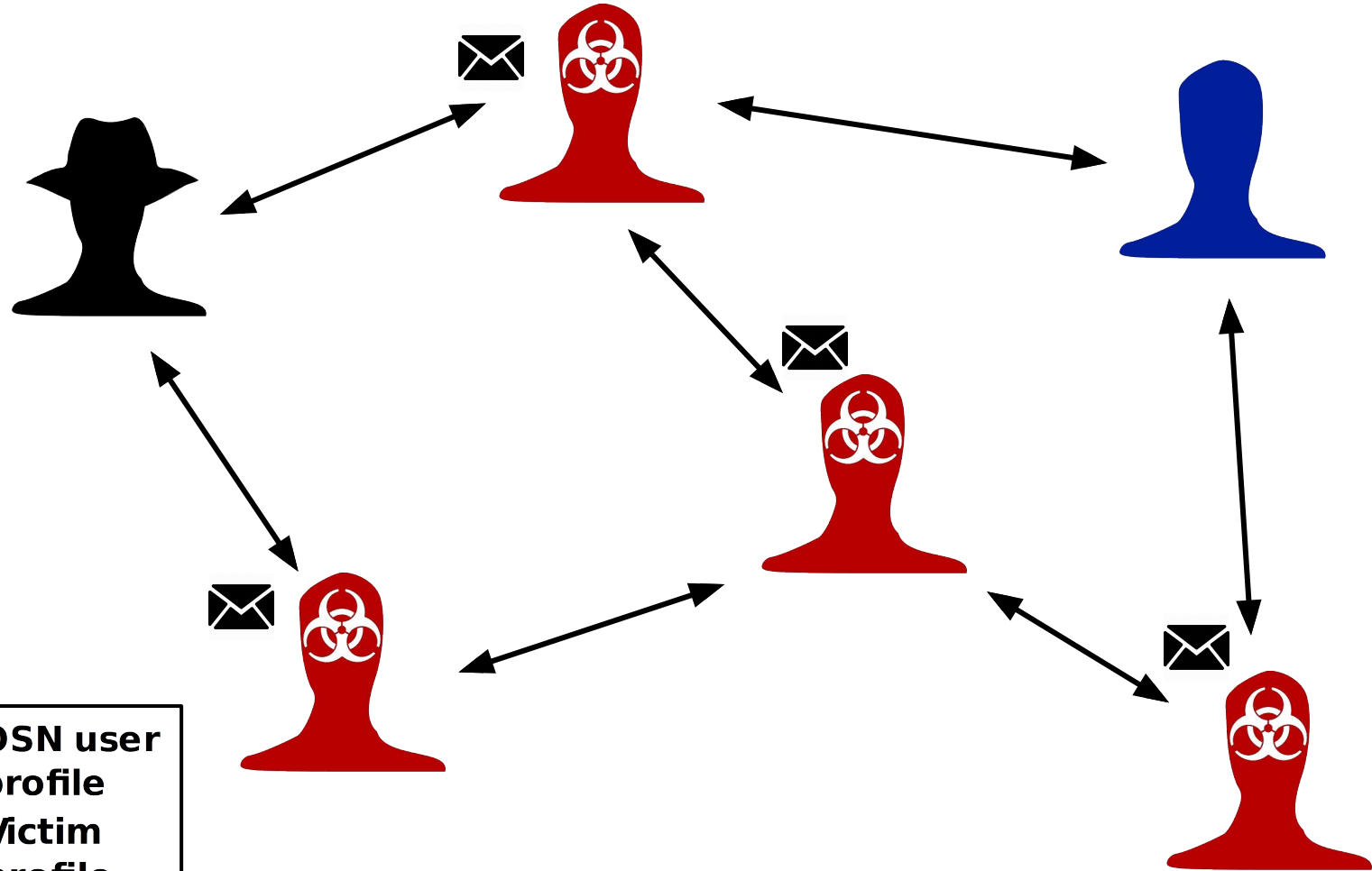





Propagation Example



	OSN user profile
	Victim profile
	Botmaster account

Propagation Example



	OSN user profile
	Victim profile
	Botmaster account

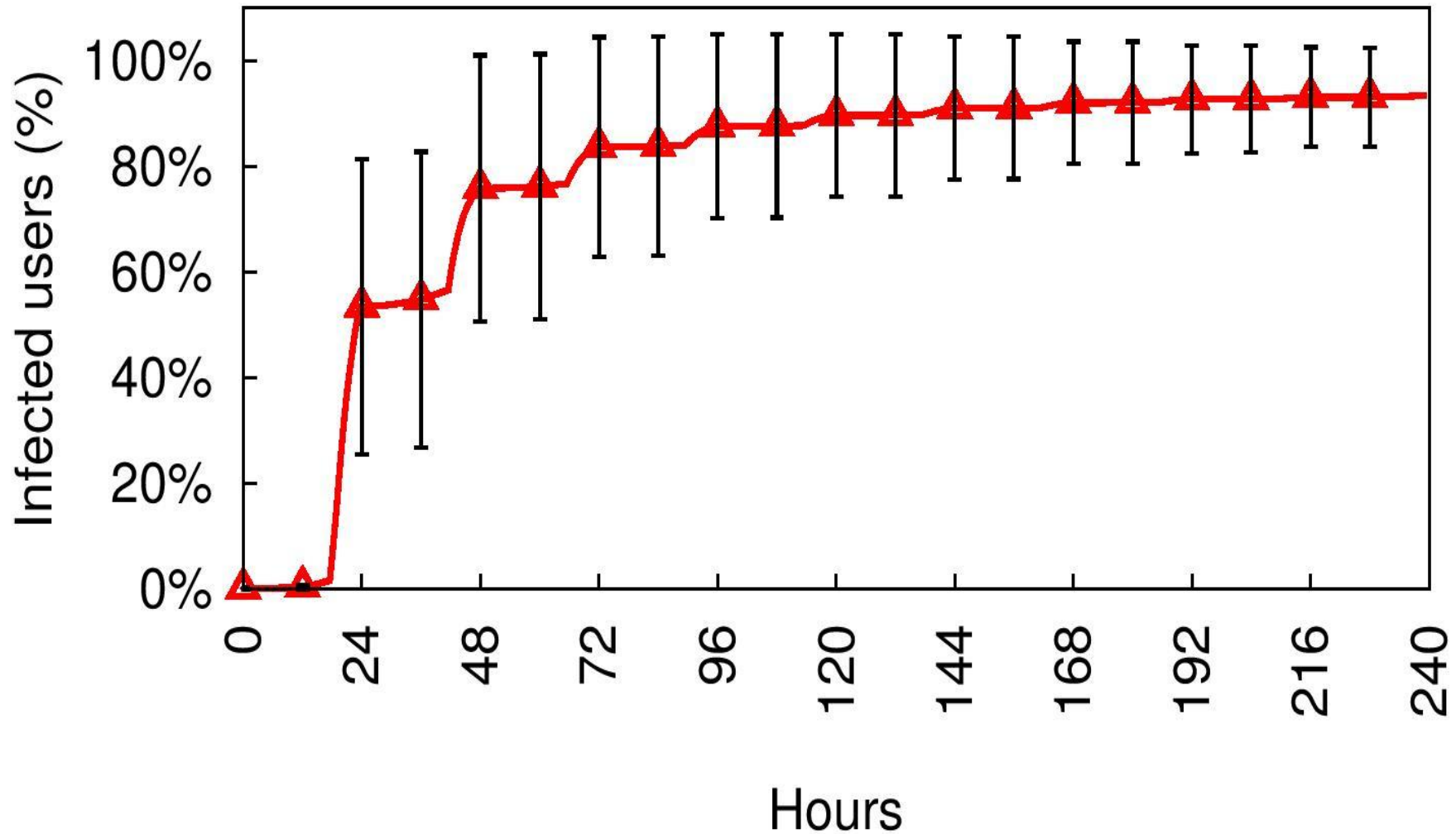
- C&C undetectability *small addition to existing network traffic*
- Unawareness by users *unicode steganography*
- Resilience *against node removals*
- Confidentiality *symmetric encryption*
- Signed commands *prevent botnet takeovers*
- Reliability *shown by experimental evaluation*

Measure **propagation speed** for C&C messages using a real OSN graph

WOSN **Facebook** dataset

Procedure:

1. **Infection**
2. **Message retransmission**
 - *Average online time*
 - *Average number of posts per day*
 - *Considering only “relevant friends”*



OSN: No straightforward detection solution
(*character blacklisting not convenient*)

Network: Undetectable with state-of-the-art detection techniques

Acceptable time needed for message spreading

Future Work

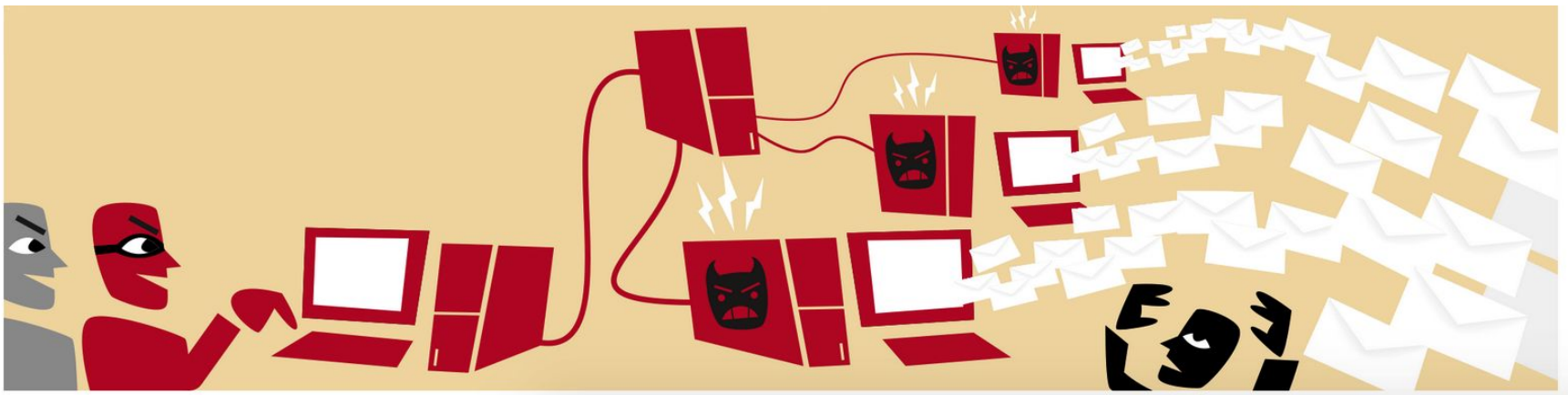
- **Empirically prove undetectability**
- **Measure *control messages* spreading**
- **Analyze the impact of multiple botmasters**
- **Investigate on mobile applications**

Questions?



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Thank you



What is *Boten Anna*?



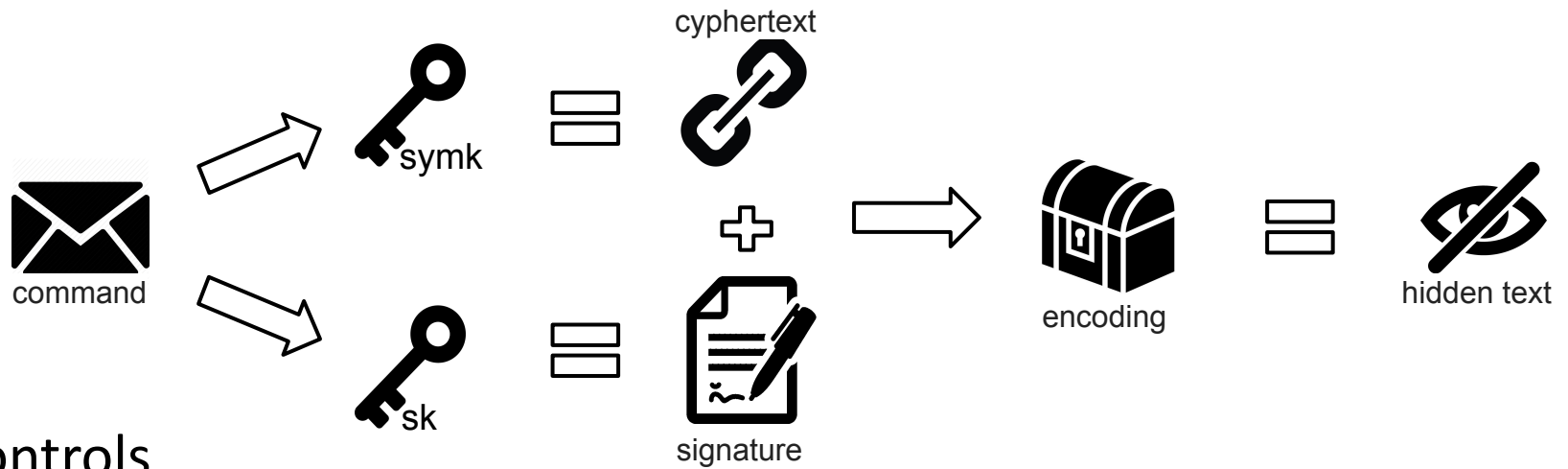
A joke on

- ELIZA, the famous computer “*chatterbot*”
- a 10-years-old swedish song about Anna, an IRC “*boten*” who turns out to be a real girl...

```
* lubo` has quit IRC (Ping tim  
* Tookie^away has quit IRC (Pi  
<Dj-Jocke> Fett ös på SB 14  
<IDM> Club Mystique ikväll?  
<osjs> ksch ksch! ;)  
<BassHunter> Värst vad boten v  
* FrazeR has quit IRC (Ping ti  
<Anna^> jag är ingen bot ;)  
jag är en väldig|
```

... While in ELISA people are hidden bots

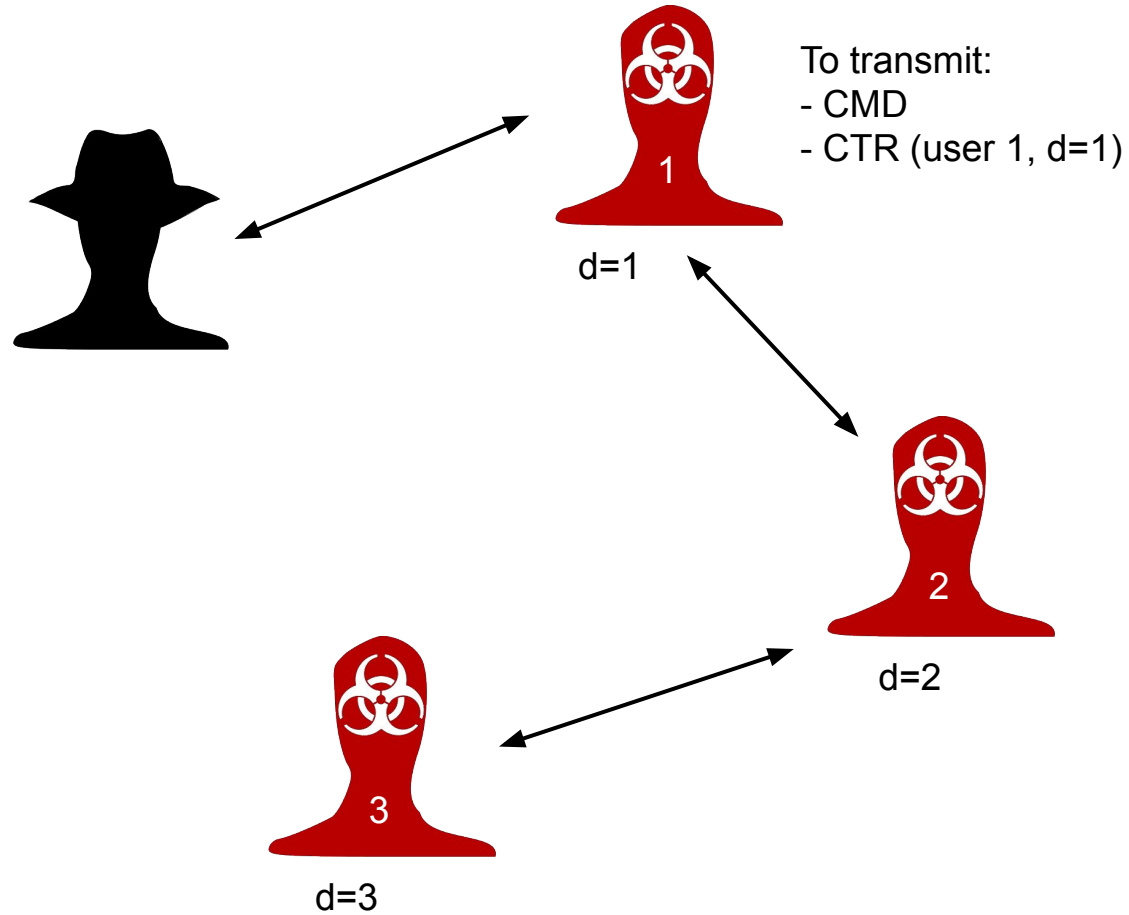
Commands



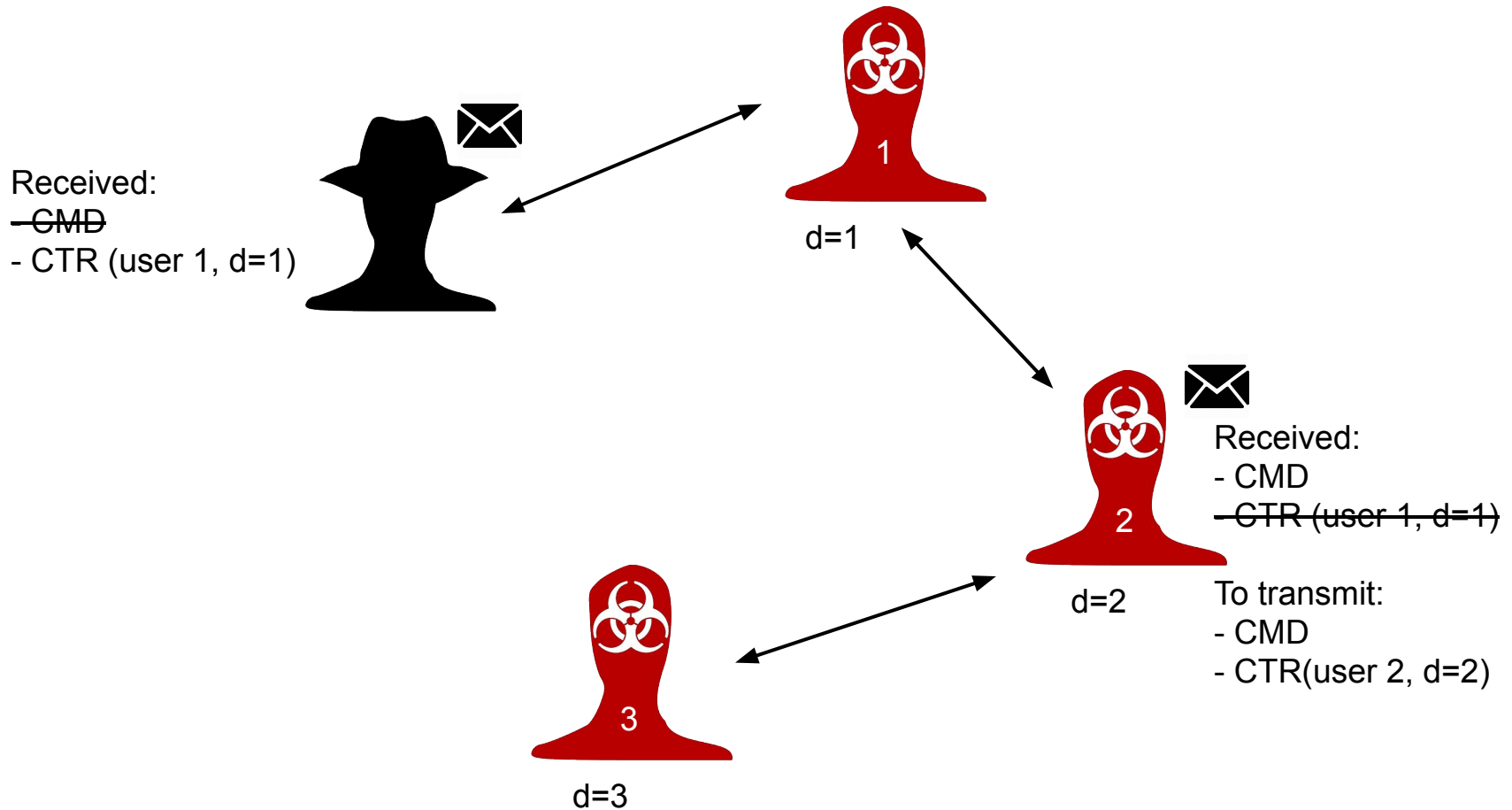
Controls



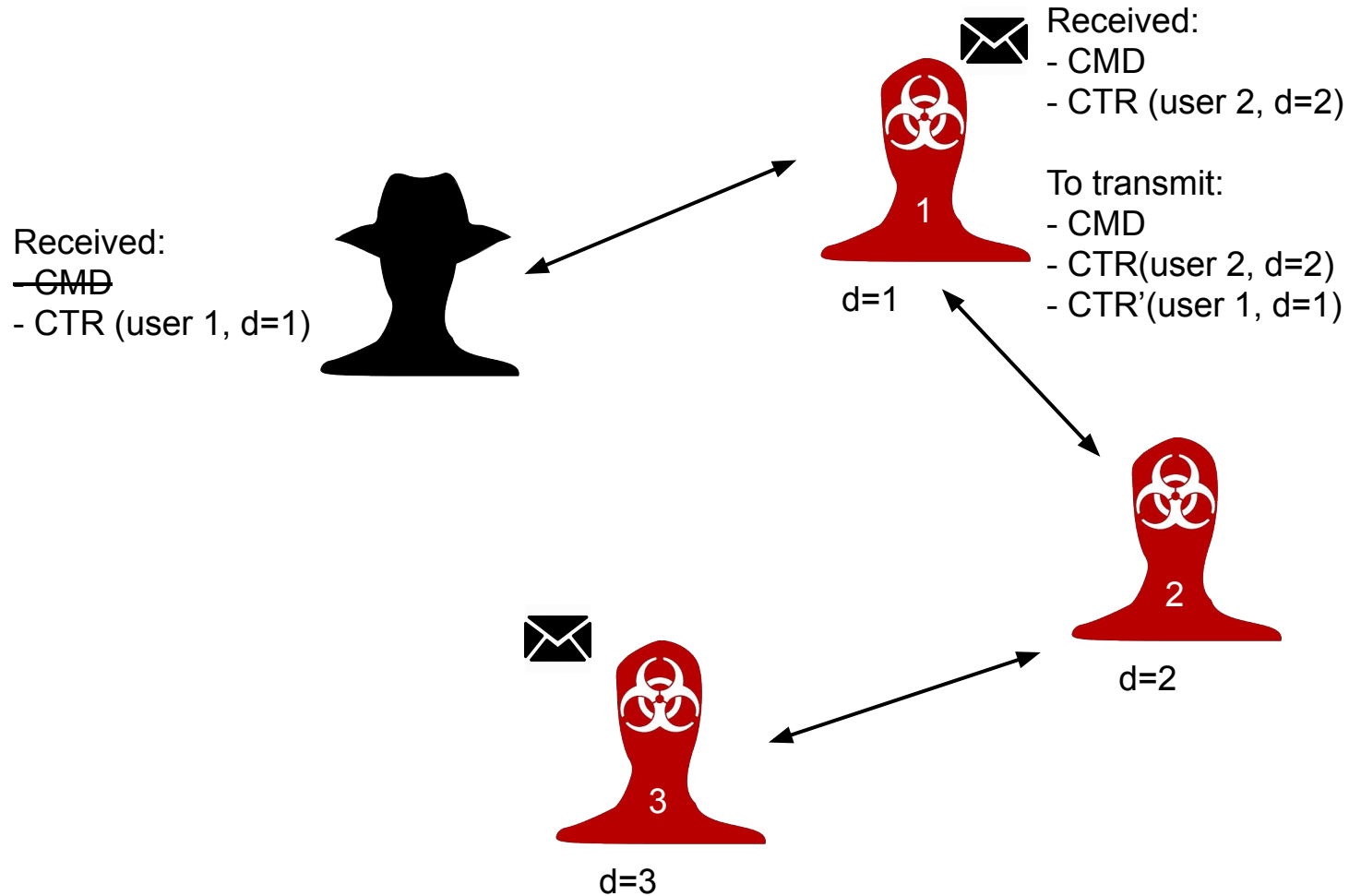
Control message propagation



Control message propagation



Control message propagation

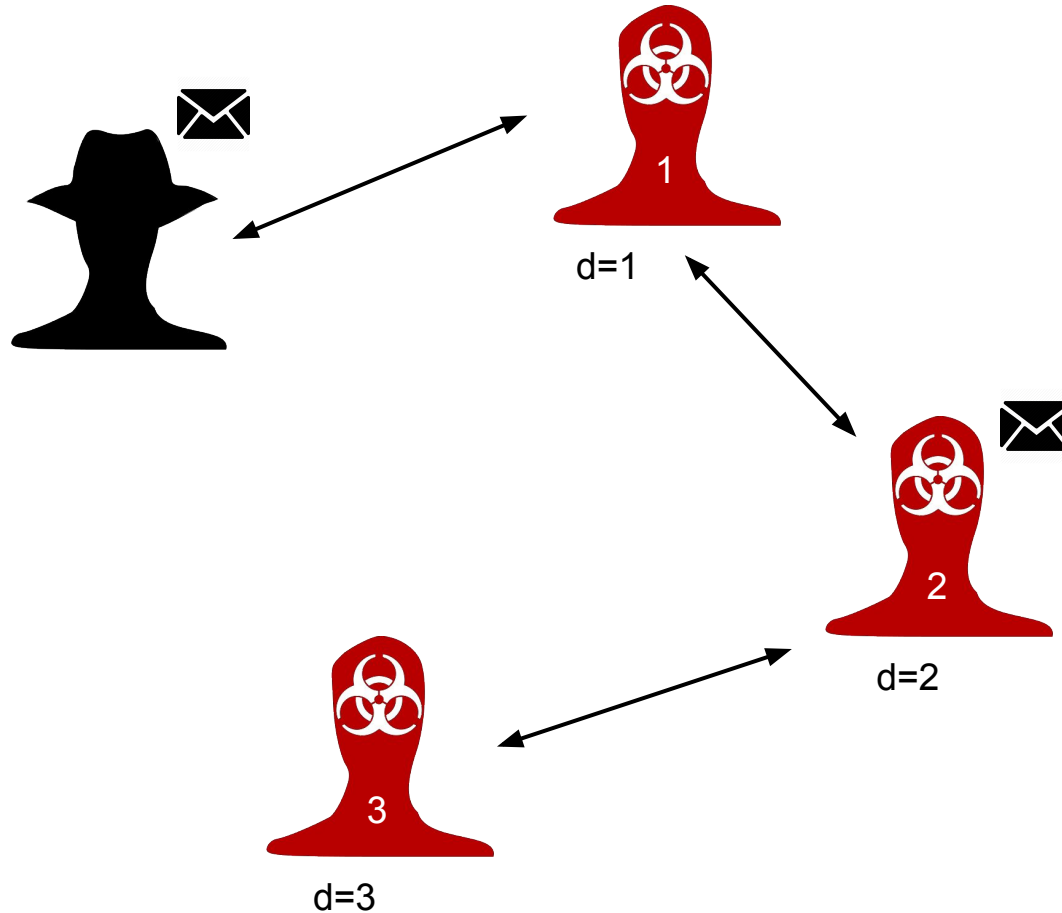


Control message propagation



Received:

- GMD
- CTR (user 1, d=1)
- CTR (user 2, d=2)
- CTR'(user 1, d=1)



Alphabets



Character code	Google+	Facebook
200c	✓	✓
200d	✓	✓
2060	✓	✓
200e	✓	×
200f	✓	×
061c	✓	✓
202a	✓	×
202b	✓	×
202e	✓	×
202c	✓	×
2061	✓	✓
00ad	✓	✓
2062	✓	✓
206a	✓	✓
206c	✓	✓
206b	✓	✓
206d	✓	✓
2063	✓	✓
Character code	Google+	Facebook

Character code	Google+	Facebook
000b	✓	×
000c	✓	×
2028	✓	×
2029	✓	×
feff	✓	×
180e	✓	✓
200b	✓	×
Character code	Google+	Facebook