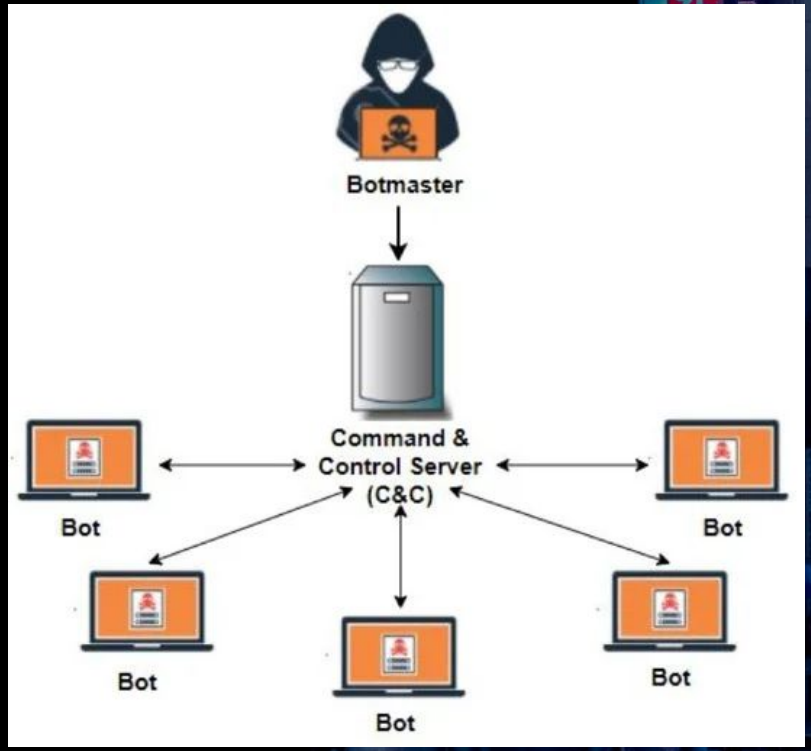
Using Wordpress comments section as a C&C for fun

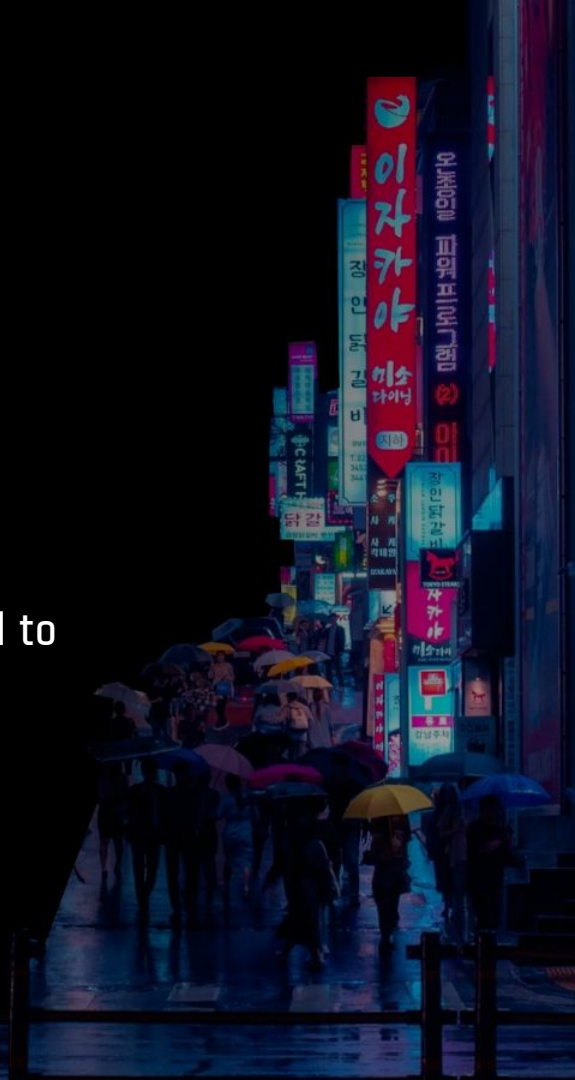
What is a C&C?

- A command-and-control [C&C] server is a computer controlled by an attacker which is used to send commands to systems compromised by malware and receive stolen data from a target network.
- Also known as C2 and CnC
- Terms:
    - Attacker = BotMaster
    - Compromised Systems = Bots

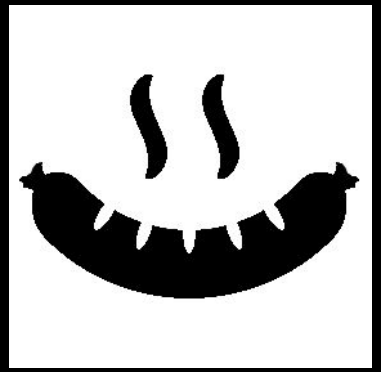


Who am I?

- Juan Karlo Licudine
  - @accidentalrebel
  - www.accidentalrebel.com
- Cyber Security Engineer
  - I help evaluate and implement cybersecurity solutions
  - Technical support
- Was a programmer/developer for 10+ years, recently switched to Cybersecurity
  - I make cybersecurity tools for defensive and offensive operations



Where it started



- I made a Remote Access Tool (RAT) called RATwurst
  - https://github.com/accidentalrebel/ratwurst
  - Uses traditional approach to C&C
    - i.e. Host server on cloud, use that as C&C server

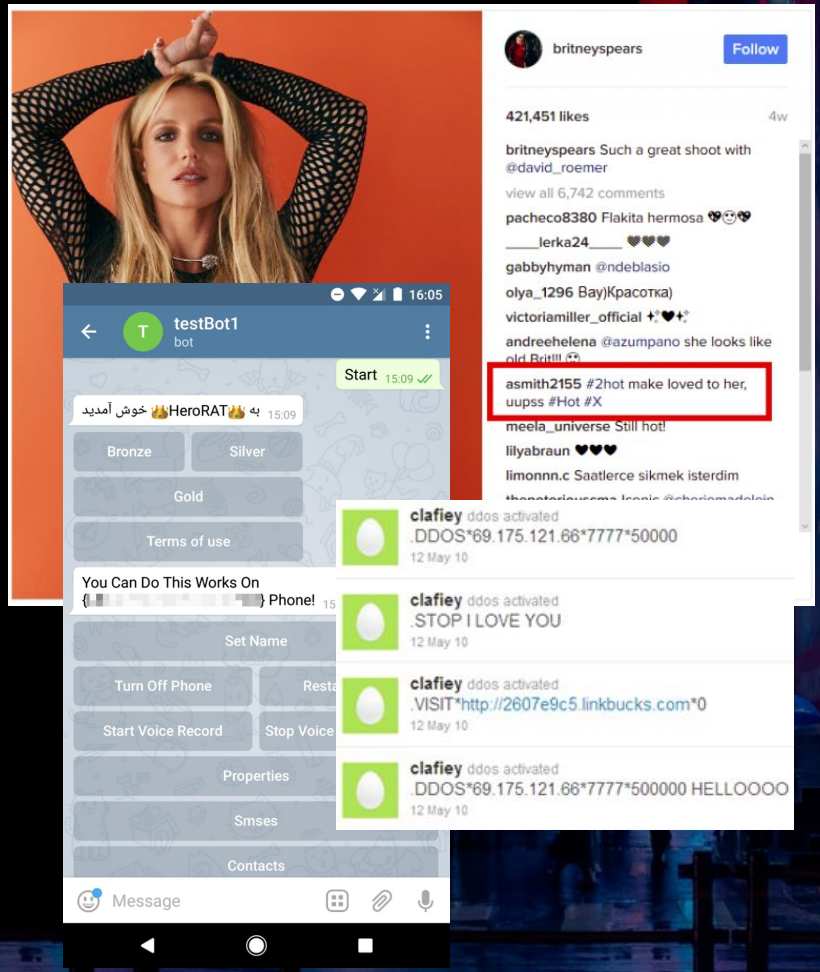
- Pursuing Evasive Custom Command & Control C3 by: Mark Ian Secretario / Renzon Cruz
  - Rootcon talk: https://www.youtube.com/watch?v=Lg-Zxtzhabc

Custom C&Cs

Threat actors have been coming up with novel ideas to use as C&Cs

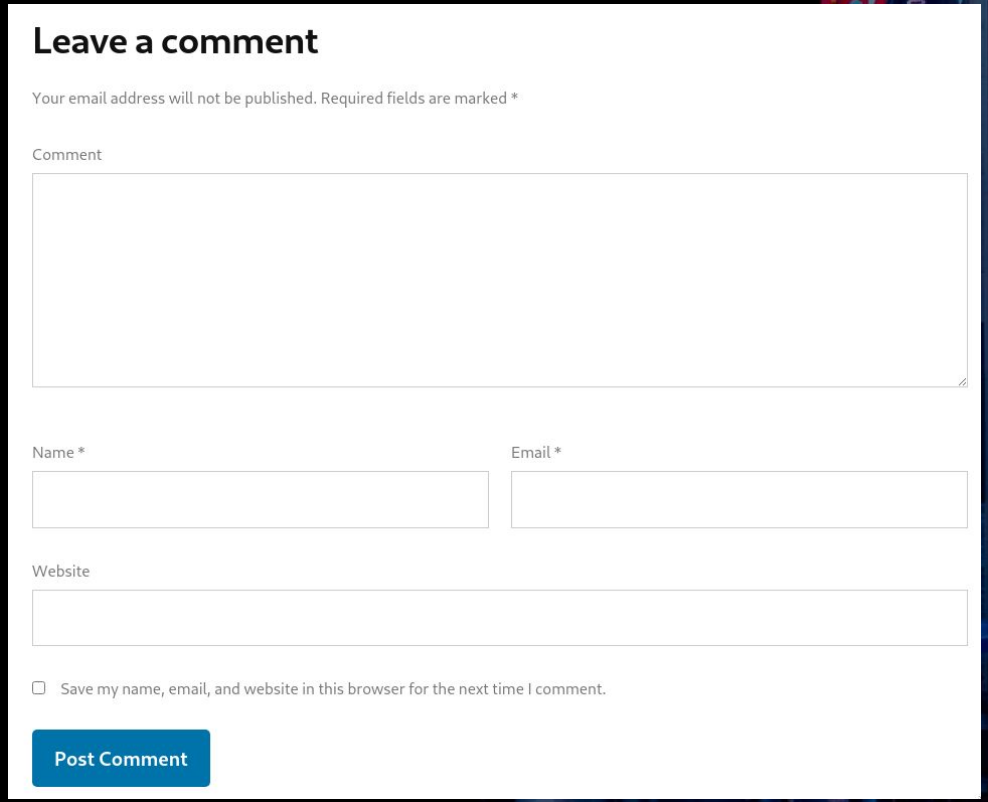
- **Instagram** - https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/
- **Telegram** - https://www.bleepingcomputer.com/news/security/telecrypt-ransomware-uses-telegram-as-candc-server/
- Outlook Mailbox - https://github.com/boku7/azureOutlookC2

I wondered what other services can be used as a C&C server?

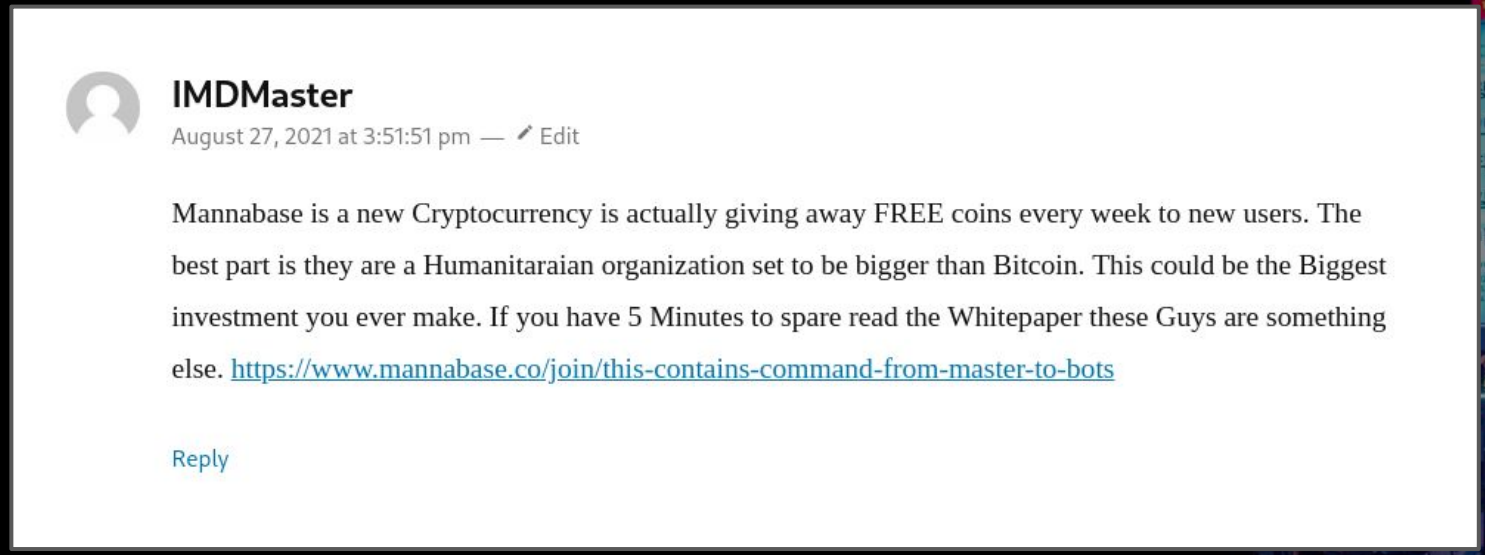


Wordpress

- Wordpress is a blogging CMS (Content Management System)
- It is used (almost) everywhere
- I've worked with Wordpress a lot when I was a web developer
- Opensource
- You can leave a comment anonymously 



The idea



IMDMaster

August 27, 2021 at 3:51:51 pm — Edit

Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

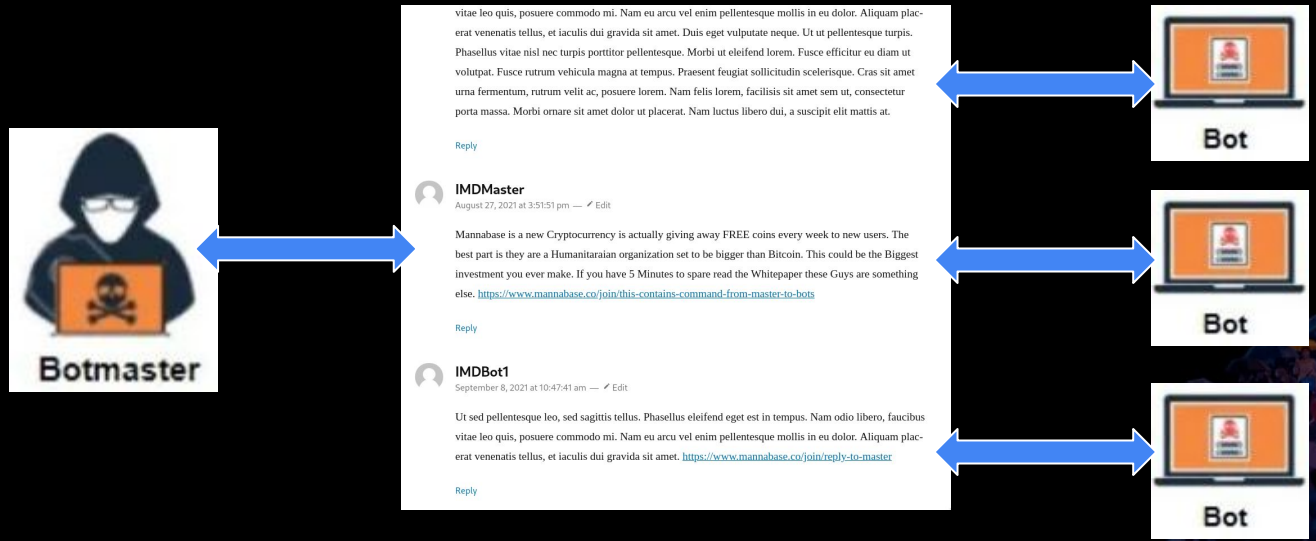
Reply

The process:

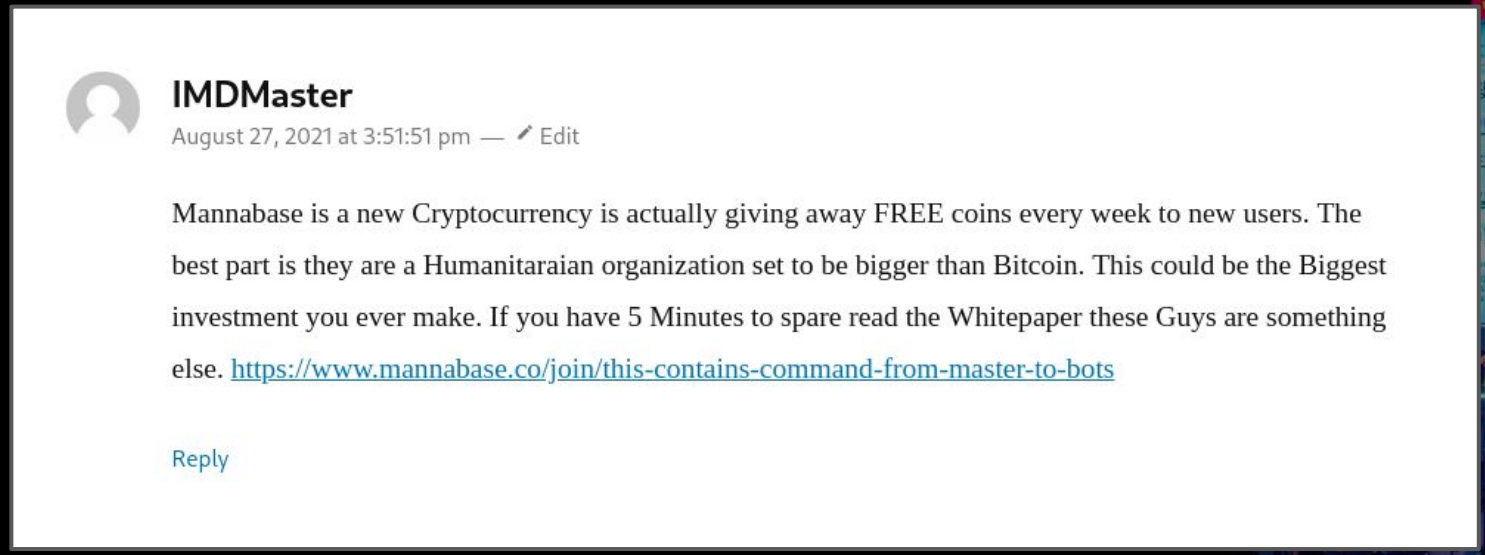
- Master sends command to a random blog in the form of a spam comment
- Bots monitor the comments section for messages from the Master
- If a message is found, parse the command

The idea

- The Wordpress blog becomes the communication channel!



Not making it too obvious



IMDMaster

August 27, 2021 at 3:51:51 pm — Edit

Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

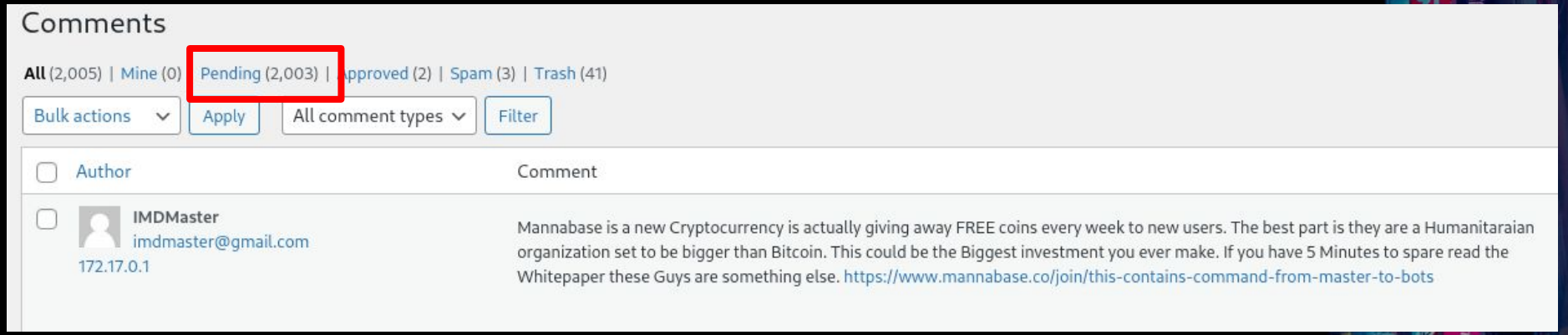
Encrypting the message:

- https://www.mannabase.co/join/this-contains-command-from-master-to-bots

For example, using rot13:

- https://www.mannabase.co/join/guvf-pbagnvaf-pbzznaq-sebz-znfgre-gb-obg

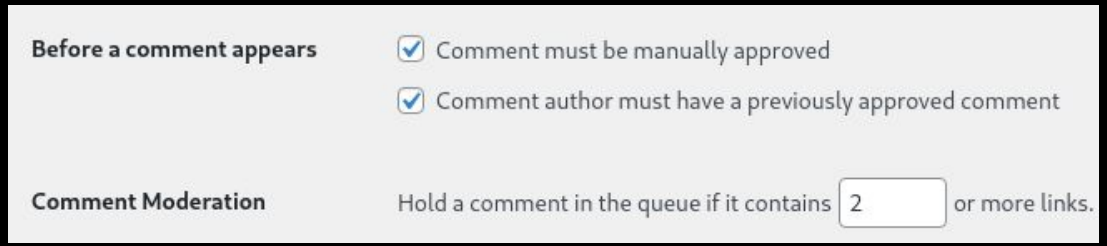
“Everyone hates spam”



- Owners of blogs would take some steps to stop further spam by turning on auto-moderation
  - Wherein a comment is automatically sent to a moderation queue for review
  - No one else can see it, not unless it has been approved by the blog owner

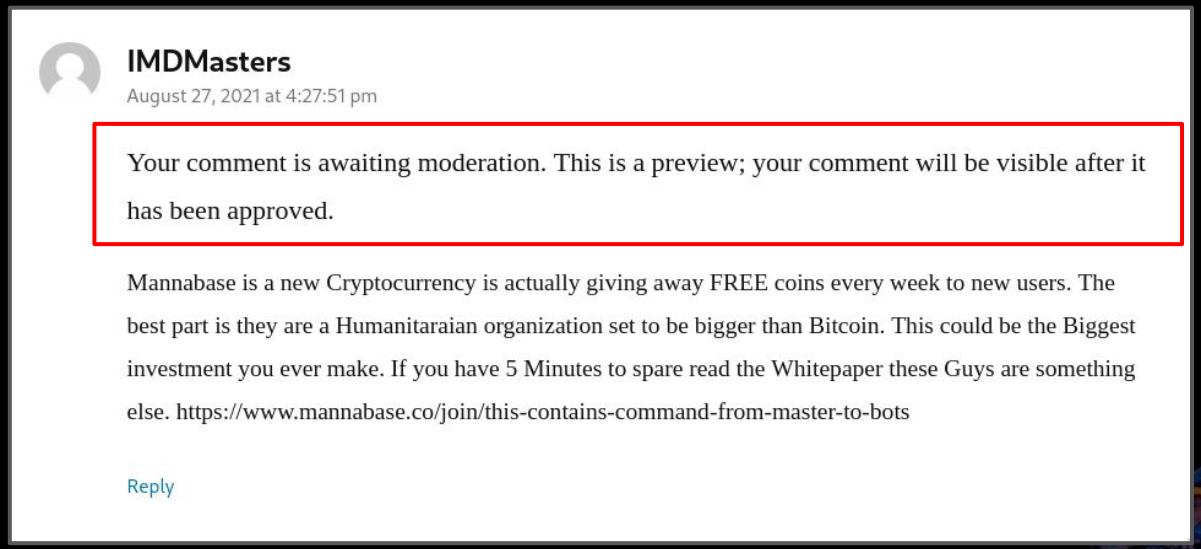
The initial idea (v1) - Downsides

- For this idea to work, a blog needs to be unmoderated
- Moderation is turned on by default!



- Really hard to look for blogs that are unmoderated

To the drawing board



IMDMasters
August 27, 2021 at 4:27:51 pm

Your comment is awaiting moderation. This is a preview; your comment will be visible after it has been approved.

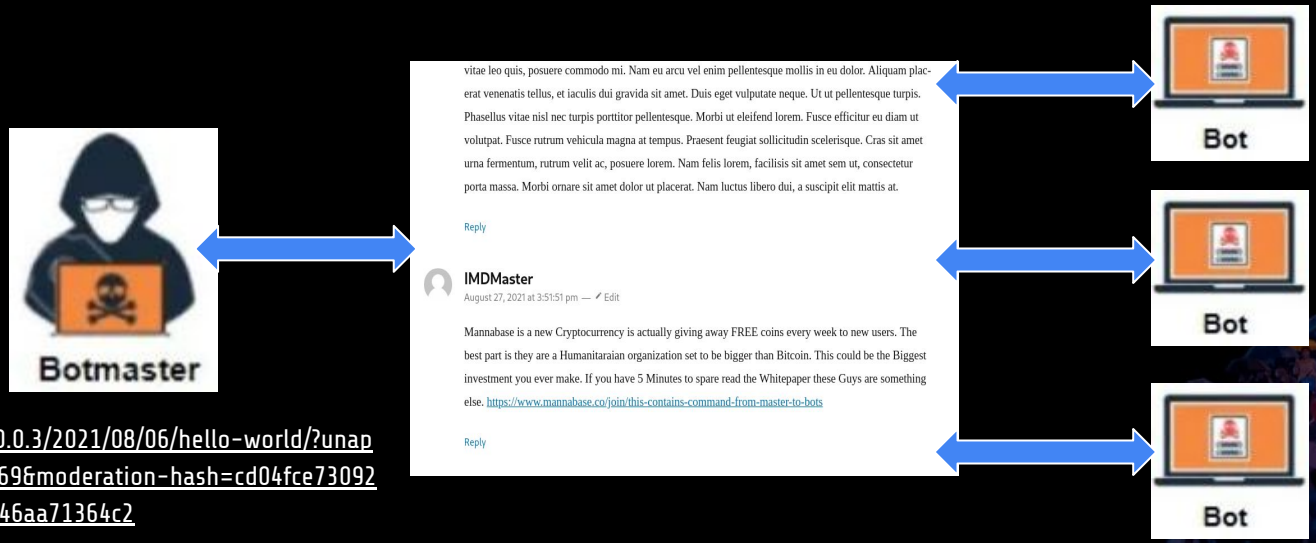
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

- When a comment is held for moderation, a unique preview link is generated: http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2
- The preview comment will be visible and accessible as long as you have the URL
- This preview will expire and disappear after 10 minutes

The problem

- Master sends a command to the blog
- Comment gets auto-moderated, a preview link is generated

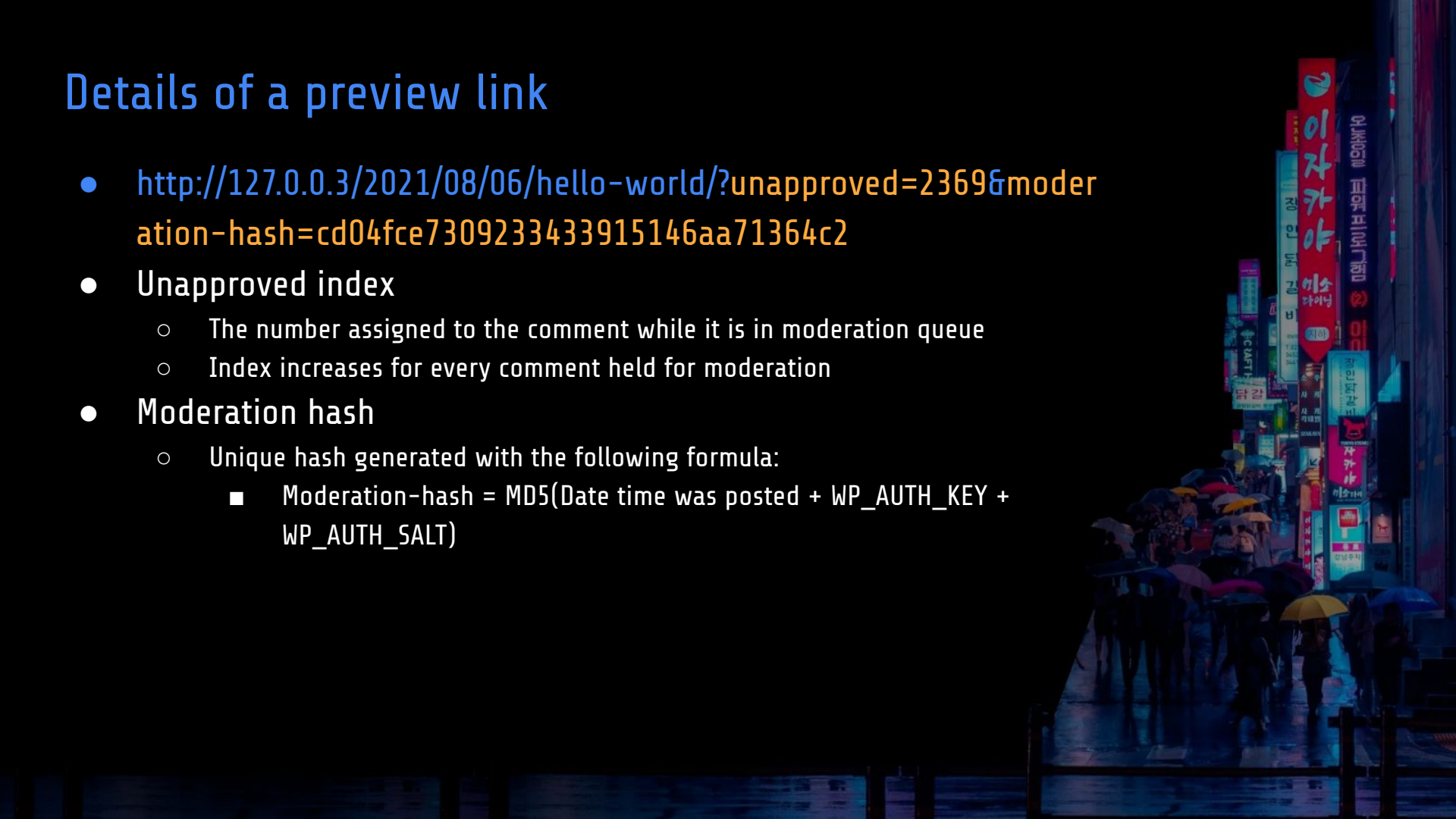


- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2

- How will the bots know the preview URL of the command?
  - Generate the preview link themselves!

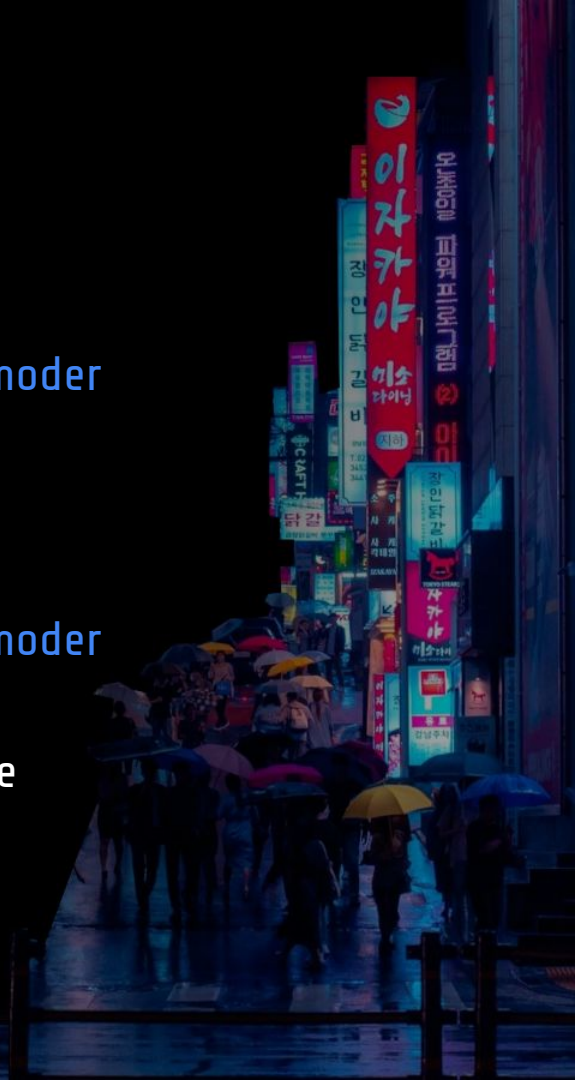
Details of a preview link

- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce73092334339151 46aa71364c2
- Unapproved index
  - The number assigned to the comment while it is in moderation queue
  - Index increases for every comment held for moderation
- Moderation hash
  - Unique hash generated with the following formula:
    - Moderation-hash = MD5(Date time was posted + WP_AUTH_KEY + WP_AUTH_SALT)



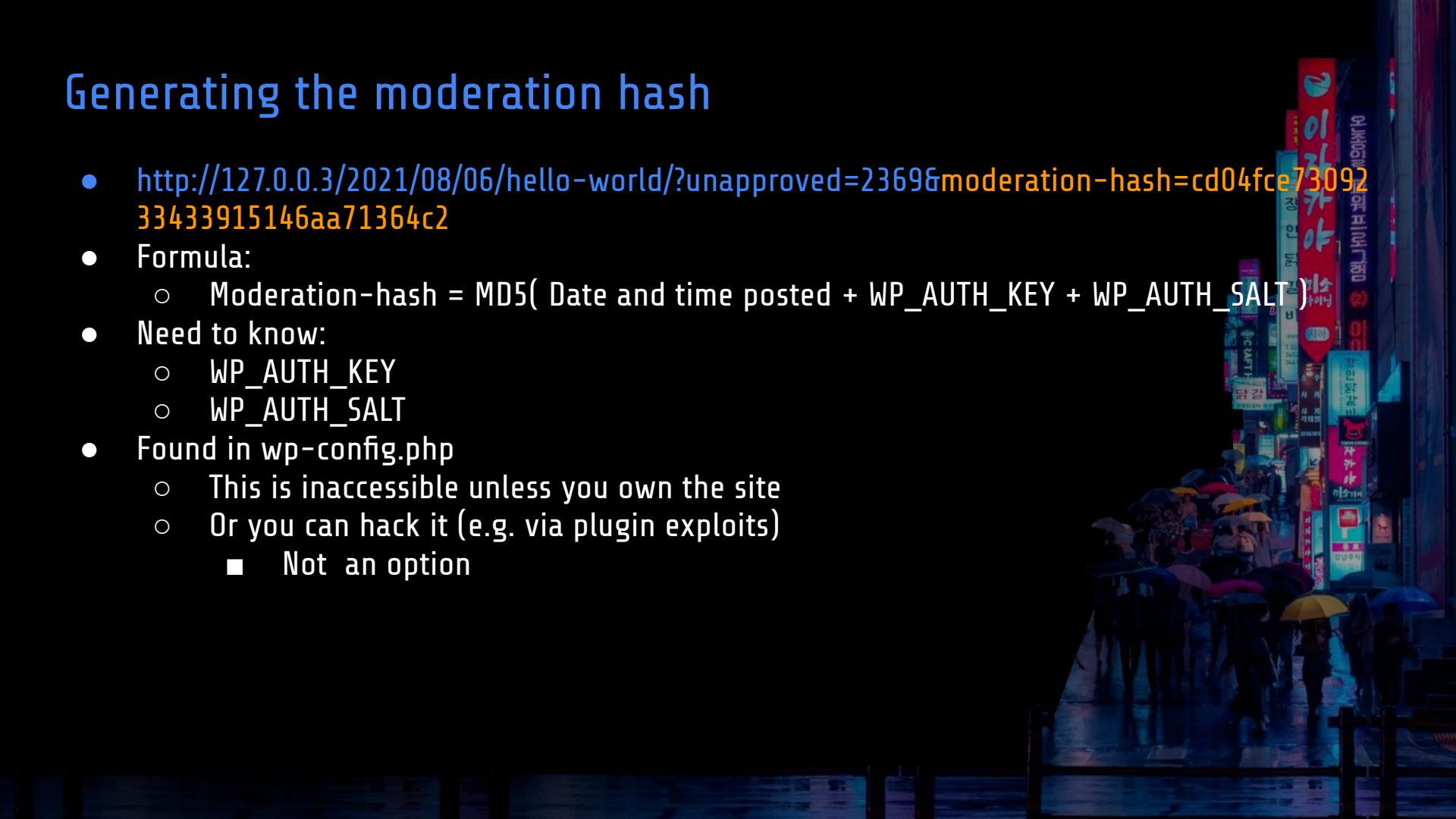
Determining the unapproved index

- Botmaster posts comment
- Botmaster receives preview link: http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce73092334339151 46aa71364c2
- Bot posts a comment
- Bot receives a preview link: http://127.0.0.3/2021/08/06/hello-world/?unapproved=2370&moderation-hash=cd04fce73092334339151 46aa71364c2
- Bot's comment is 2370, therefore Botmaster's comment will be <2370
    - This can be brute-forced!



Generating the moderation hash

- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2
- Formula:
  - Moderation-hash = MD5(Date and time posted + WP_AUTH_KEY + WP_AUTH_SALT)
- Need to know:
  - WP_AUTH_KEY
  - WP_AUTH_SALT
- Found in wp-config.php
  - This is inaccessible unless you own the site
  - Or you can hack it (e.g. via plugin exploits)
    - Not an option



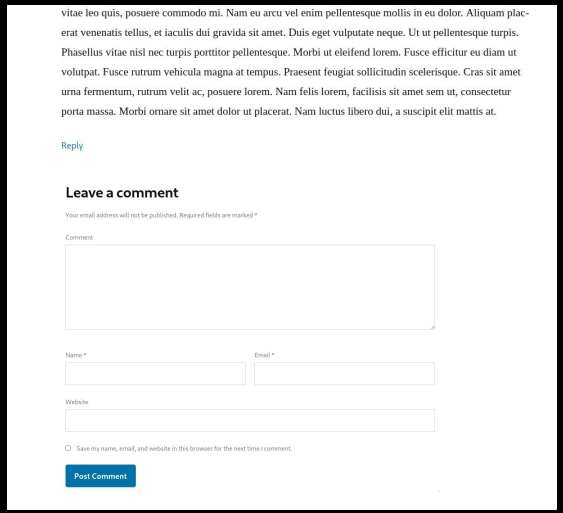
~~Generating~~ Getting the moderation hash

- Instead of computing the hash, what if bots post a comment as the same time as the master?
- The bots and master would get the same moderation-hashes because all of them posted at 12:20!
  - Seconds are discarded
    - 12:20:00 and 12:20:01 would have the same moderation hash

The improved idea (v3)

Current time: 12:11:00

- Prepare the message to send.
- Next time-window is 12:20



vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

Leave a comment

Your email address will not be published. Required fields are marked *

Comment

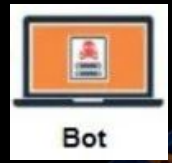
Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

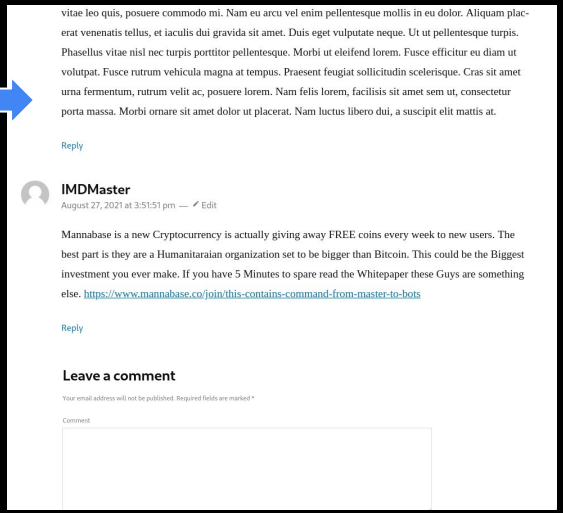
Post Comment



- Prepare to receive message
- Next time-window is 12:20

The improved idea (v3)

Current time: 12:20:00



vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — ✎ Edit

Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

Leave a comment

Your email address will not be published. Required fields are marked *

Comment

- Botmaster sends message and receives preview link
- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2

The improved idea (v3)

Current time: 12:20:01

- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

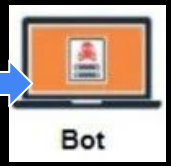
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

Reply



- Bot sends message and receives preview link
- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2370&moderation-hash=cd04fce7309233433915146aa71364c2

The improved idea (v3)

Current time: 12:20:02

- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

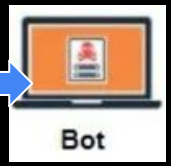
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

Reply



- Gets HTML Response:
- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2367&moderation-hash=cd04fce7309233433915146aa71364c2
- 404 - Not found

The improved idea (v3)

Current time: 12:20:03

- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

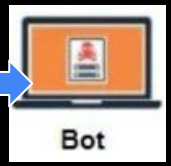
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

Reply



- Gets HTML Response:
- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2368&moderation-hash=cd04fce7309233433915146aa71364c2
- 404 - Not found

The improved idea (v3)

Current time: 12:20:04

- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

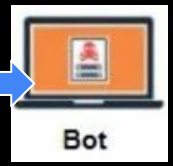
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

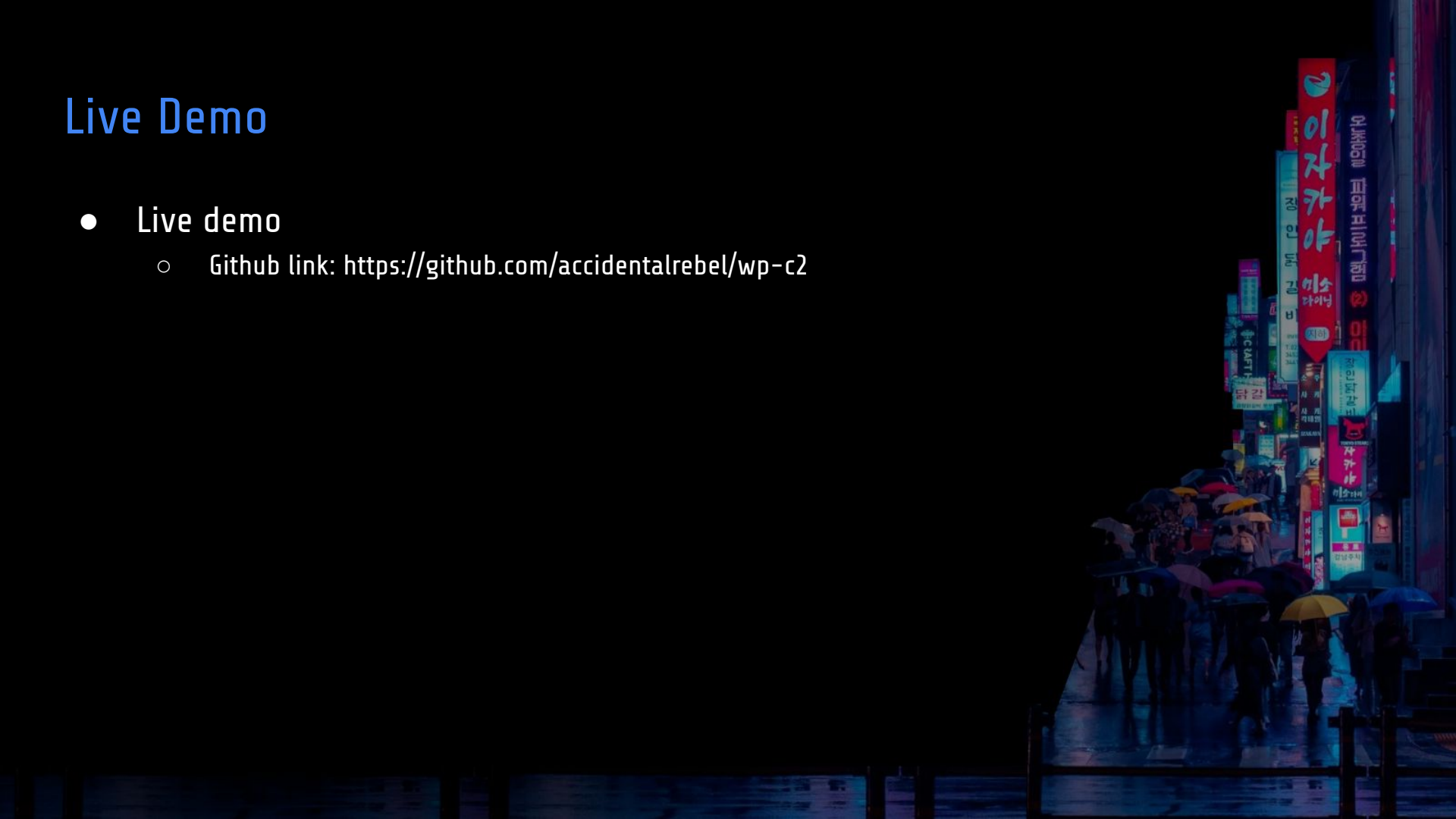
Reply



- Gets HTML Response:
- http://127.0.0.3/2021/08/06/hello-world/?unapproved=2369&moderation-hash=cd04fce7309233433915146aa71364c2
- 200 - OK
- Found message!

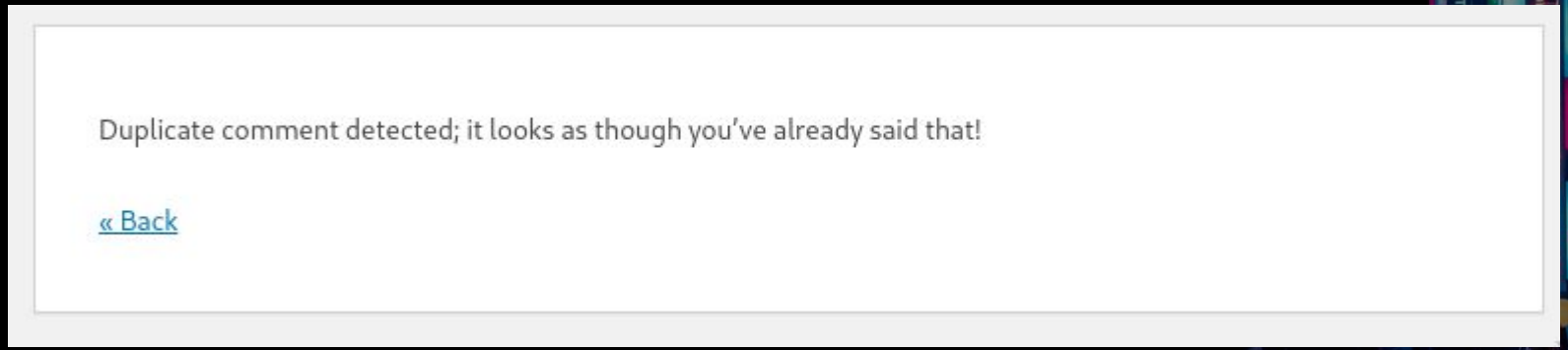
Live Demo

- Live demo
  - Github link: https://github.com/accidentalrebel/wp-c2



Acknowledging receipt

- When a comment has already been posted. A message is shown.
- We can use this as a way to confirm if a message has been sent.
- For example, when confirming if BotMaster has received exfiltrated data



Acknowledging receipt

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

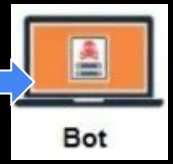
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

Reply



- Sends exfiltrated data with identifier “ABC123”

Acknowledging receipt

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

Reply

- Received exfiltrated data.
- Posting comment containing “ABC123 received”

Acknowledging receipt

vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. Duis eget vulputate neque. Ut ut pellentesque turpis. Phasellus vitae nisl nec turpis porttitor pellentesque. Morbi ut eleifend lorem. Fusce efficitur eu diam ut volutpat. Fusce rutrum vehicula magna at tempus. Praesent feugiat sollicitudin scelerisque. Cras sit amet urna fermentum, rutrum velit ac, posuere lorem. Nam felis lorem, facilisis sit amet sem ut, consectetur porta massa. Morbi ornare sit amet dolor ut placerat. Nam luctus libero dui, a suscipit elit mattis at.

Reply

IMDMaster
August 27, 2021 at 3:51:51 pm — Edit

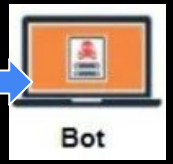
Mannabase is a new Cryptocurrency is actually giving away FREE coins every week to new users. The best part is they are a Humanitaraian organization set to be bigger than Bitcoin. This could be the Biggest investment you ever make. If you have 5 Minutes to spare read the Whitepaper these Guys are something else. https://www.mannabase.co/join/this-contains-command-from-master-to-bots

Reply

IMDBot1
September 8, 2021 at 10:47:41 am — Edit

Ut sed pellentesque leo, sed sagittis tellus. Phasellus eleifend eget est in tempus. Nam odio libero, faucibus vitae leo quis, posuere commodo mi. Nam eu arcu vel enim pellentesque mollis in eu dolor. Aliquam placerat venenatis tellus, et iaculis dui gravida sit amet. https://www.mannabase.co/join/reply-to-master

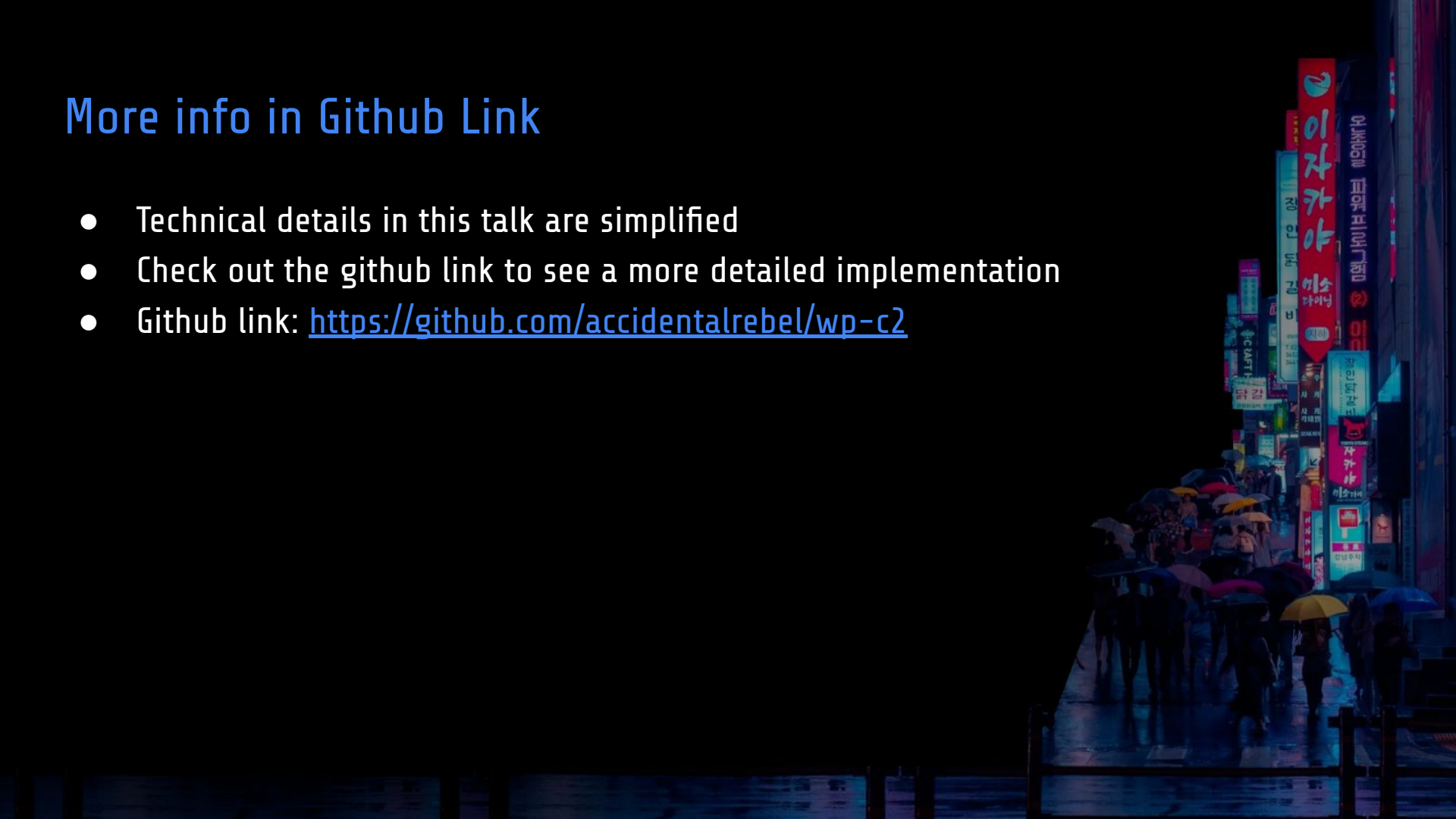
Reply



- Posts a comment with identifier ““ABC123 received”
- If response returns “Duplicate comment detected” , it means botmaster received it
- If not, Bot resends the exfiltrated data

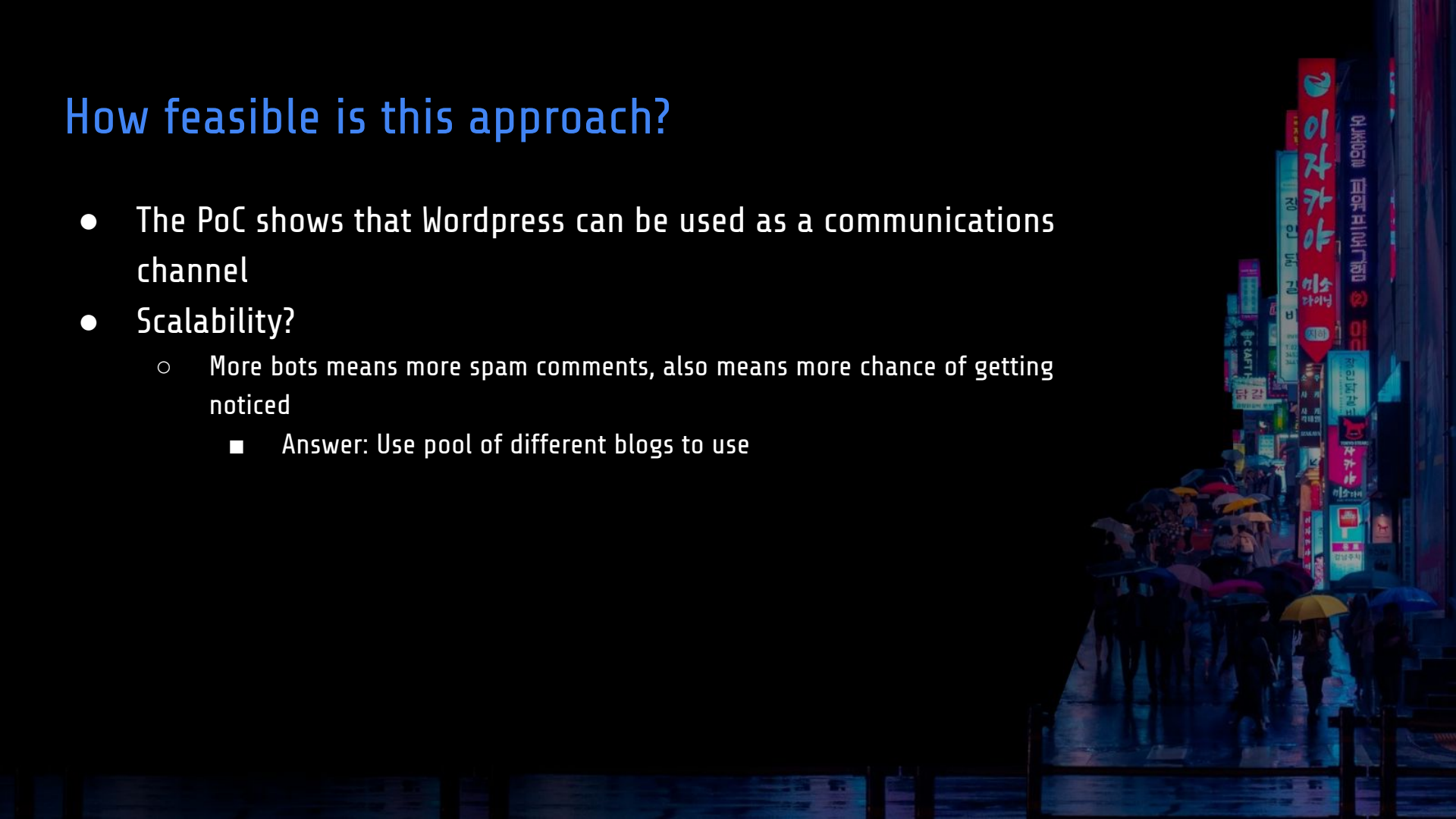
More info in Github Link

- Technical details in this talk are simplified
- Check out the github link to see a more detailed implementation
- Github link: https://github.com/accidentalrebel/wp-c2



How feasible is this approach?

- The PoC shows that Wordpress can be used as a communications channel
- Scalability?
  - More bots means more spam comments, also means more chance of getting noticed
    - Answer: Use pool of different blogs to use



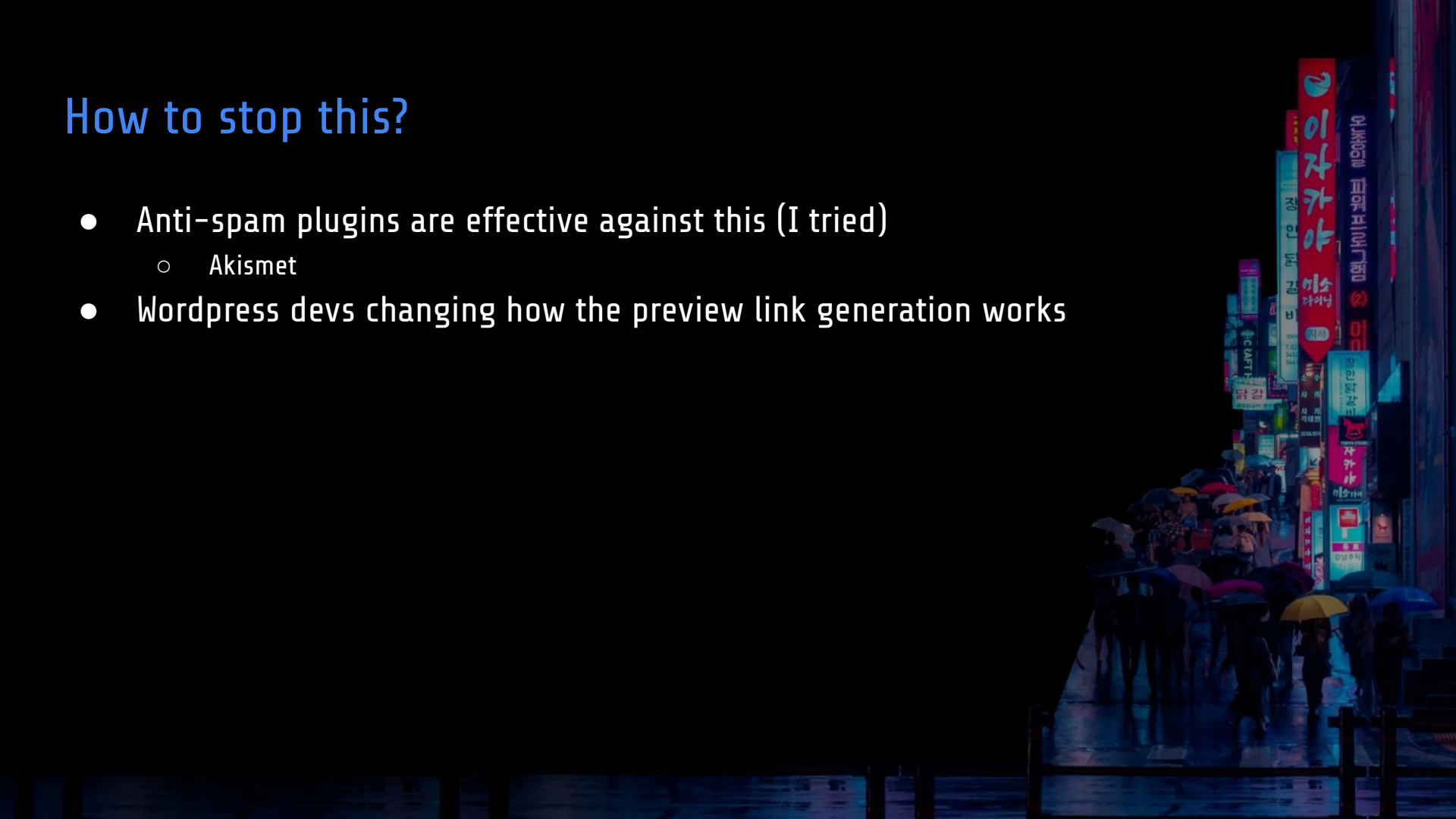
How feasible is this approach?

- Detectability?
  - Auto-moderation can be to our advantage

  - Defenders can look for frequent and constant
    - Answer: Change the communication intervals, add randomization, or a time-table that bot Master and Bot clients know of
    - Answer: Use a pool of different blogs to use

How to stop this?

- Anti-spam plugins are effective against this (I tried)
  - Akismet
- Wordpress devs changing how the preview link generation works



Summary

- Wordpress can be a viable option to use a C&C server
- Upsides
  - Lots of blogs to use as channels
  - No cost for the attacker
  - No sign ups / No accounts
- Downsides
  - Delays - Have to wait for timeslots
  - Difference in timing can mess things up
  - Timing issues - If the server replies really slowly

Thank you very much!

- Karlo Licudine (@accidentalrebel)
  - www.accidentalrebel.com
  - github.com/accidentalrebel
  - https://github.com/accidentalrebel/wp-c2