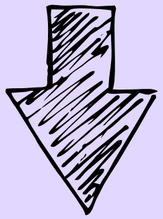
LA SEGURIDAD EN EL LAYER 0

Pablo Sabbatella

defy Education

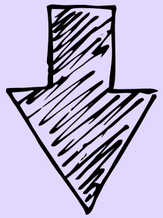
Traditional security: robar bases de datos > venderlas o utilizarlas

(dificil)



Ransomware: atacar sistemas > rescate en crypto

(más fácil)

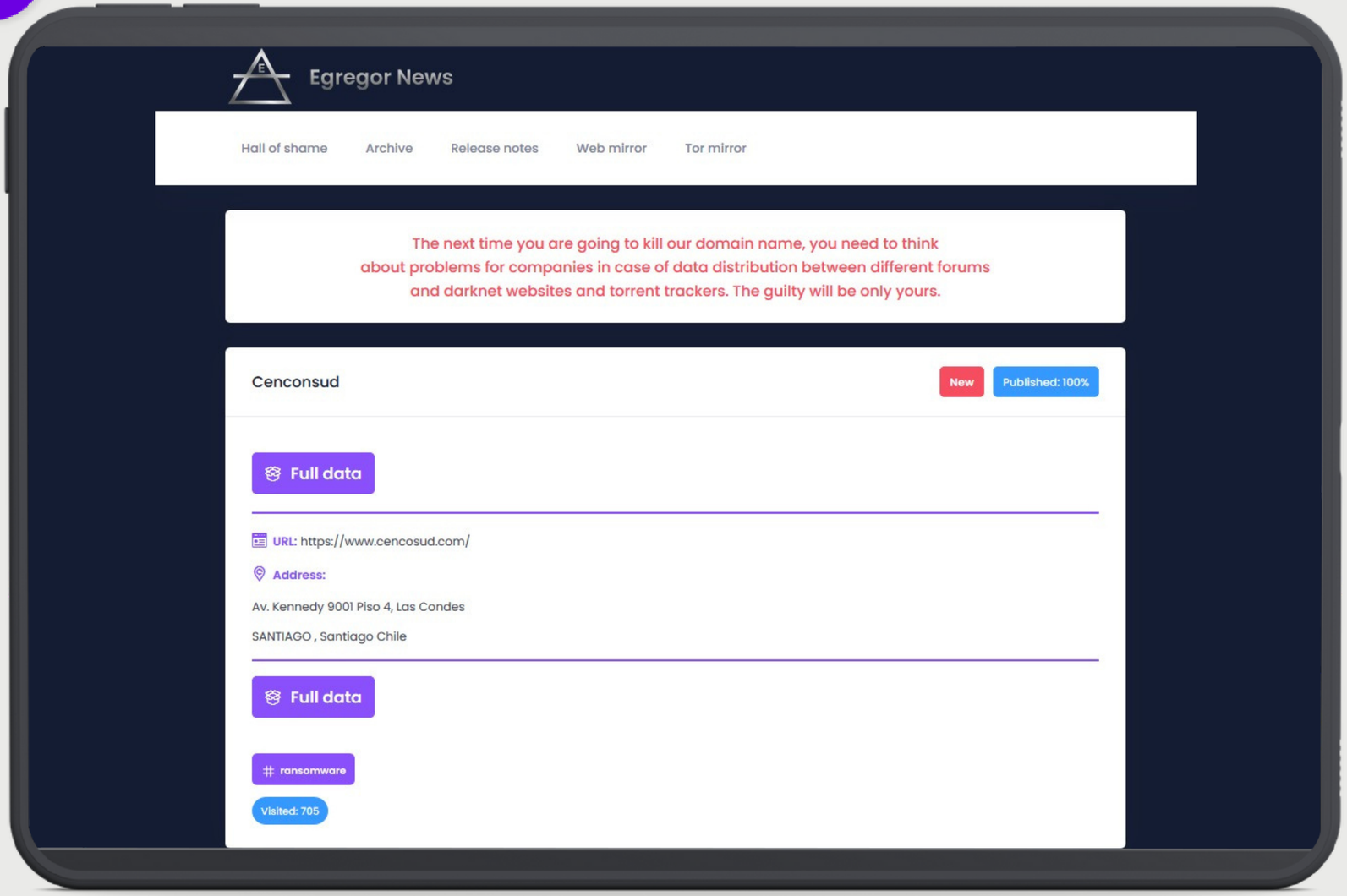


Blockchain security: atacar DeFi > botín $

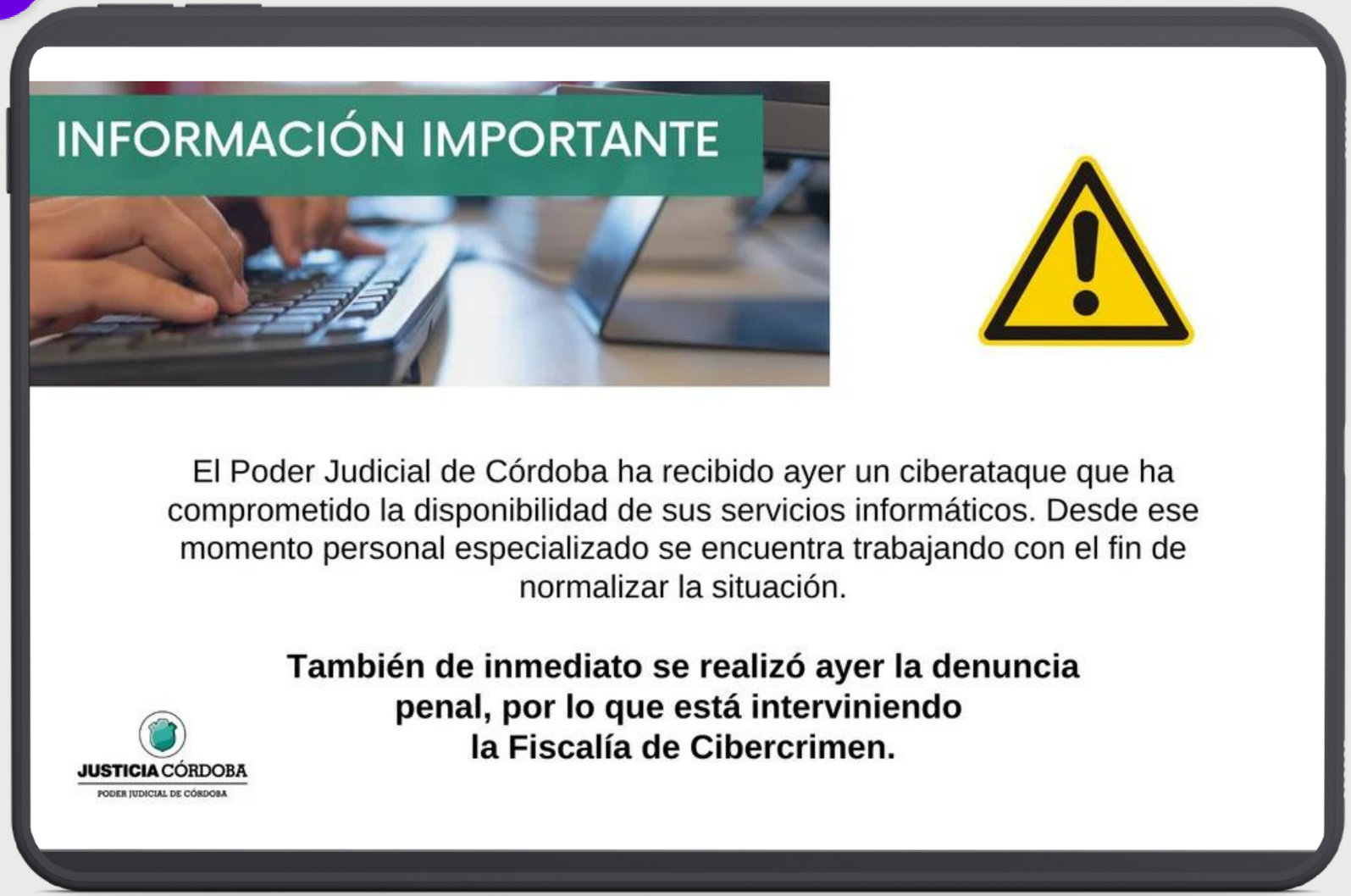
(más fácil y jugoso)

defy EDUCATION

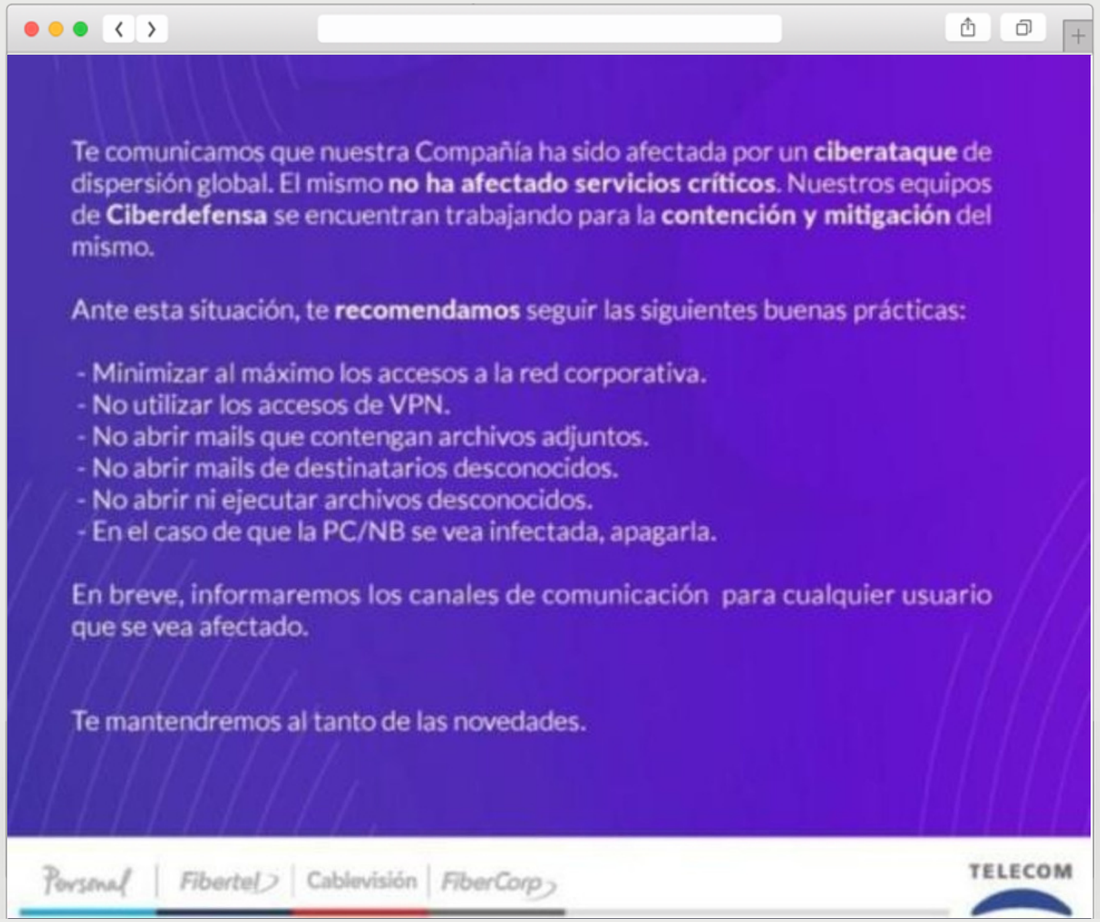
ROBO DE DBS

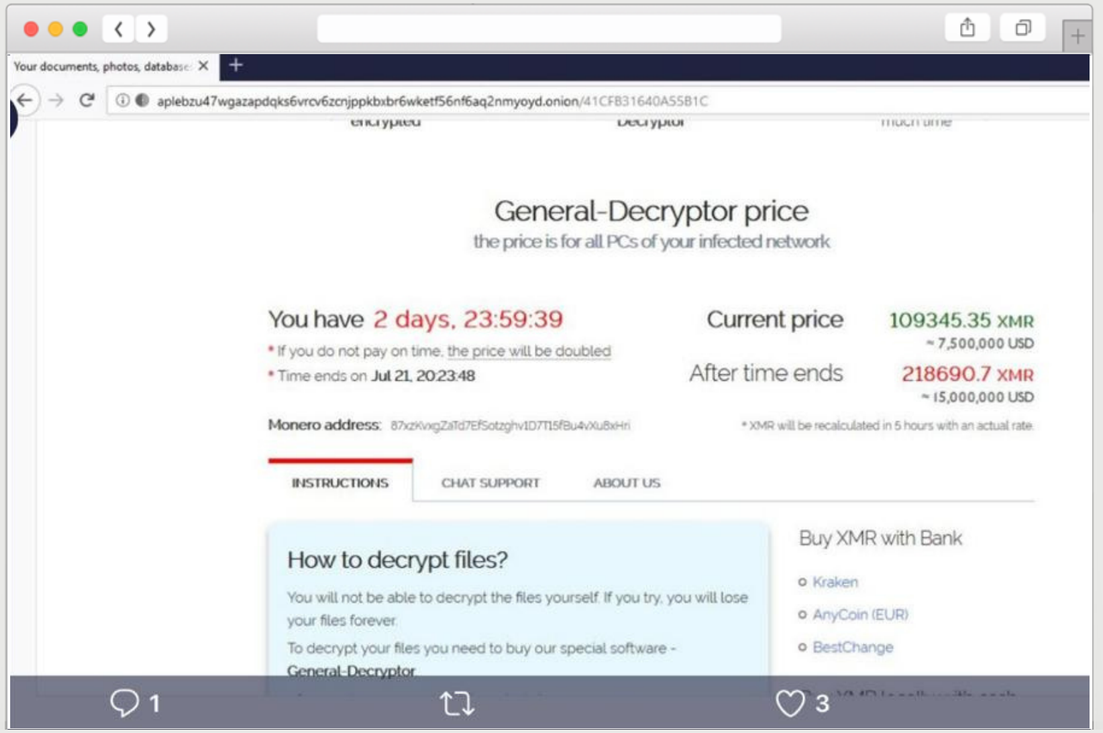

Egregor News
Hall of shame
Archive
Release notes
Web mirror
Tor mirror
The next time you are going to kill our domain name, you need to think
about problems for companies in case of data distribution between different forums
and darknet websites and torrent trackers. The guilty will be only yours.
Cenconsud
New
Published: 100%
Full data
URL: https://www.cencosud.com/
Address:
Av. Kennedy 9001 Piso 4, Las Condes
SANTIAGO , Santiago Chile
Full data
ransomware
Visited: 705

RANSOMWARE


INFORMACIÓN IMPORTANTE
El Poder Judicial de Córdoba ha recibido ayer un ciberataque que ha comprometido la disponibilidad de sus servicios informáticos. Desde ese momento personal especializado se encuentra trabajando con el fin de normalizar la situación.
También de inmediato se realizó ayer la denuncia penal, por lo que está interviniendo la Fiscalía de Cibercrimen.
JUSTICIA CÓRDOBA
PODER JUDICIAL DE CÓRDOBA

RANSOMWARE

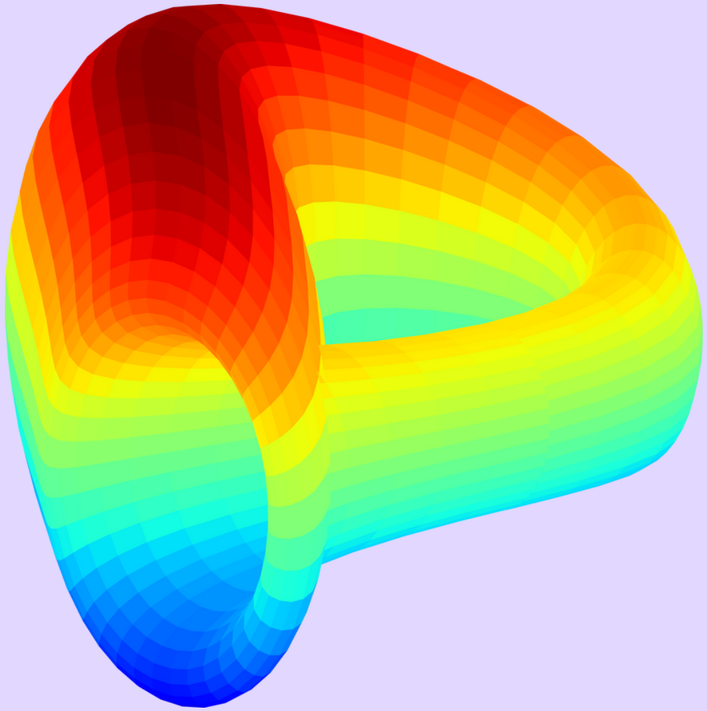

Te comunicamos que nuestra Compañía ha sido afectada por un **ciberataque** de dispersión global. El mismo **no ha afectado servicios críticos**. Nuestros equipos de **Ciberdefensa** se encuentran trabajando para la **contención y mitigación** del mismo.
Ante esta situación, te **recomendamos** seguir las siguientes buenas prácticas:
- Minimizar al máximo los accesos a la red corporativa.
- No utilizar los accesos de VPN.
- No abrir mails que contengan archivos adjuntos.
- No abrir mails de destinatarios desconocidos.
- No abrir ni ejecutar archivos desconocidos.
- En el caso de que la PC/NB se vea infectada, apagarla.
En breve, informaremos los canales de comunicación para cualquier usuario que se vea afectado.
Te mantendremos al tanto de las novedades.
Personal | Fibertel | Cablevisión | FiberCorp
TELECOM


Your documents, photos, databases
aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/41CFB31640A55B1C
General-Decryptor price
the price is for all PCs of your infected network
You have 2 days, 23:59:39
Current price
109345.35 XMR
~ 7,500,000 USD
* If you do not pay on time, the price will be doubled
* Time ends on Jul 21, 20:23:48
After time ends
218690.7 XMR
~ 15,000,000 USD
Monero address:
* XMR will be recalculated in 5 hours with an actual rate
INSTRUCTIONS
CHAT SUPPORT
ABOUT US
How to decrypt files?
You will not be able to decrypt the files yourself. If you try, you will lose your files forever.
To decrypt your files you need to buy our special software - General-Decryptor
Buy XMR with Bank
Kraken
AnyCoin (EUR)
BestChange
1
3

Es el mejor momento de la historia para hacer un scam o romper una dapp

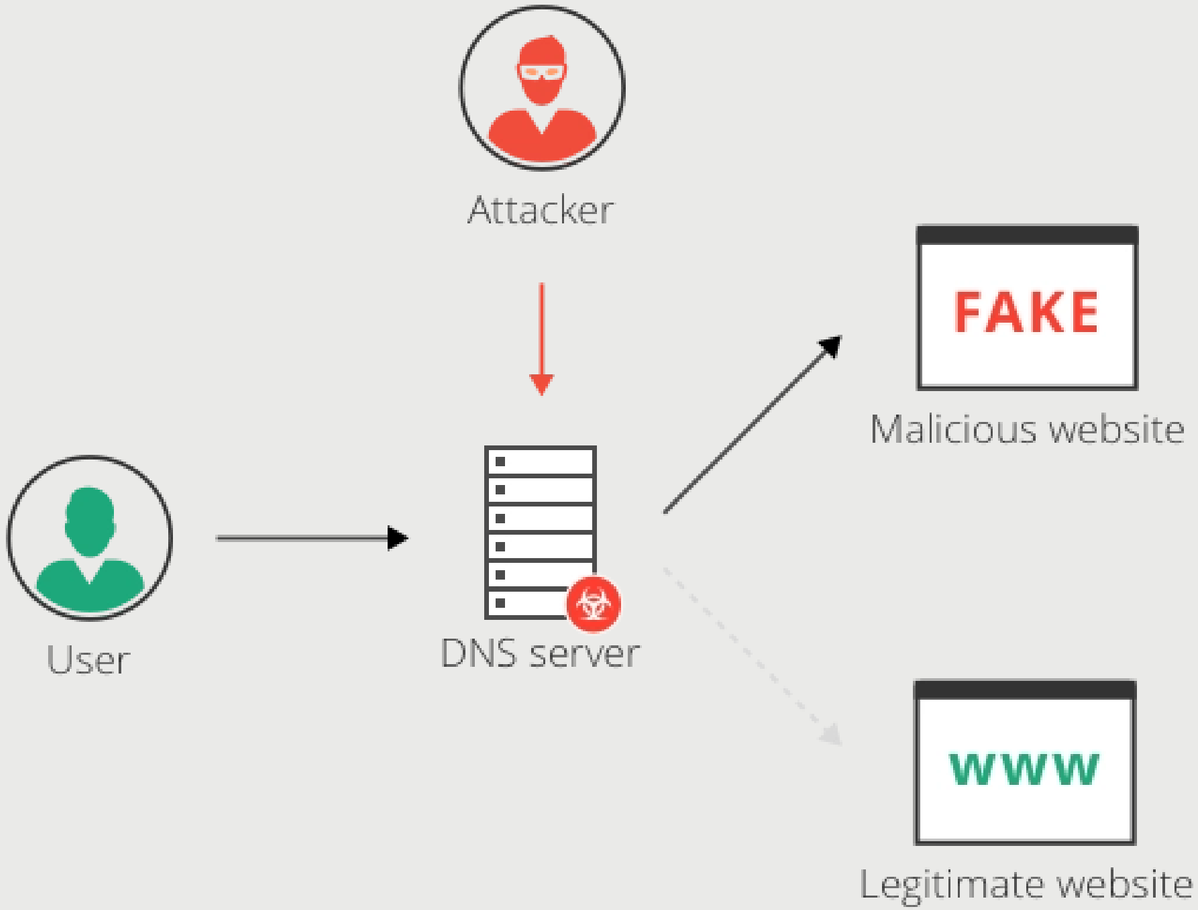
defy EDUCATION

Curve Finance: domain hijack



defy EDUCATION

CURVE FINANCE



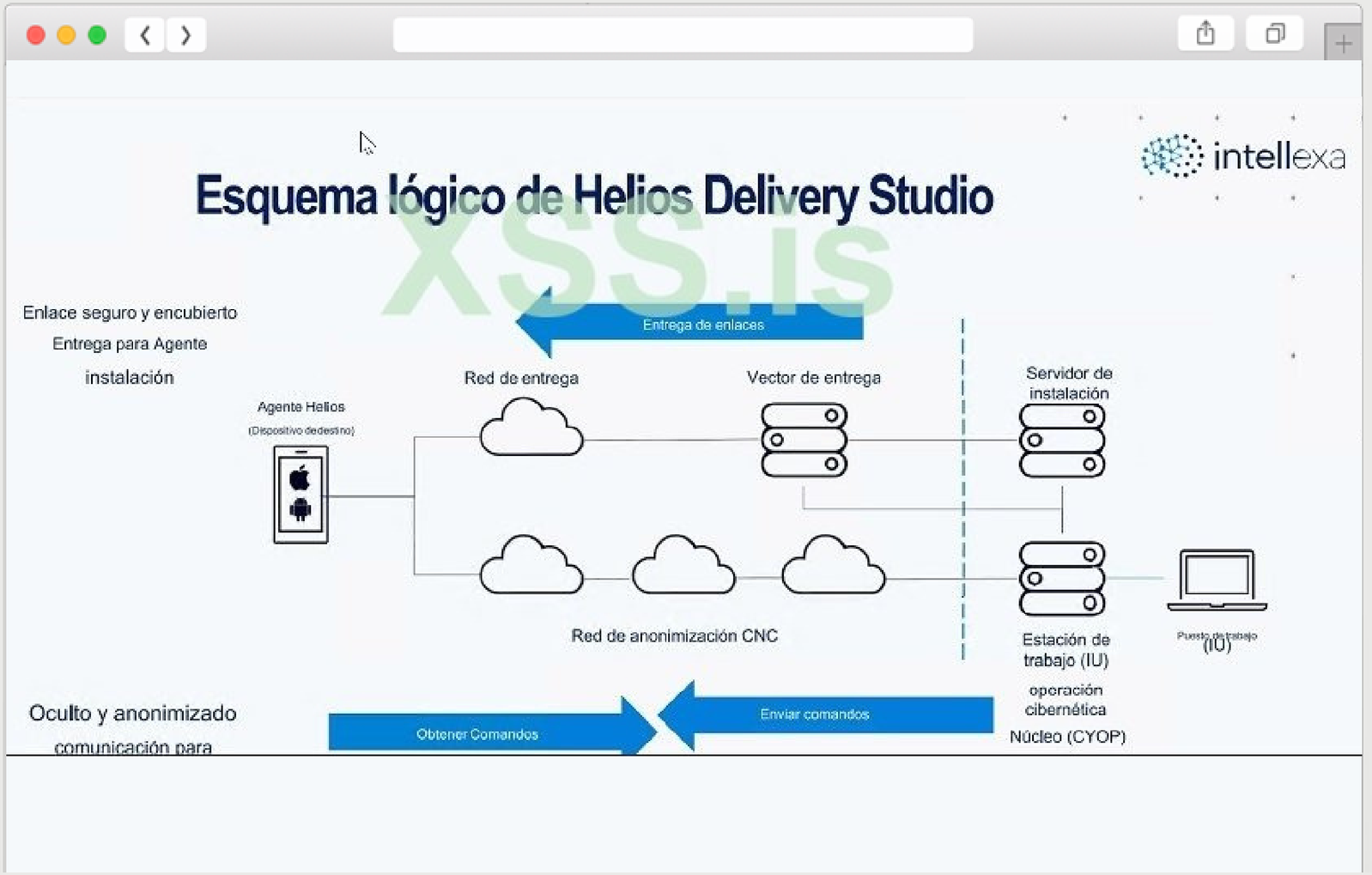
Ronin bridge: social engineering + 0day exploit

defy EDUCATION

RONIN BRIDGE

Compromised 5 out of 9 validators

0-DAYS EXPLOITS



0-DAYS EXPLOITS

91	Xiaomi Black Shark 4
92	Xiaomi Mi A3

Oppo* Devices	
Serial	Device
93	Oppo Reno6 5G
94	Oppo F11 Pro
95	Oppo A74
96	Oppo Find X2 Pro
97	Oppo Find X2 Neo
98	Oppo A73 5G
99	Oppo Reno6 Z 5G
100	Oppo Reno5 Z
101	Oppo Reno4 Pro 5G
102	Oppo Reno4 Z 5G

Huawei* Devices	
Serial	Device
103	Huawei P40 Pro
104	Huawei P30
105	Huawei P30 Pro
106	Huawei P20 Pro
107	Huawei Mate 20 Pro
108	Huawei nova 4
109	Huawei Mate 10
110	Huawei nova 5T
111	Huawei Mate 40 Pro

Honor* Devices	
Serial	Device
112	Honor View 20

* It is hereby clarified that any commitment of Intellexa to support the devices listed above, shall be valid as long as such devices contain mainstream Android distribution and Google store and Google play services with Chrome browser installed on the device.

2 Price Proposal

#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser-based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data	1	
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa. unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

PEGASUS & PREDATOR

Who has been targeted by Pegasus?

Arab royal family members

600+ politicians/ government officials

64 business executives

189 journalists

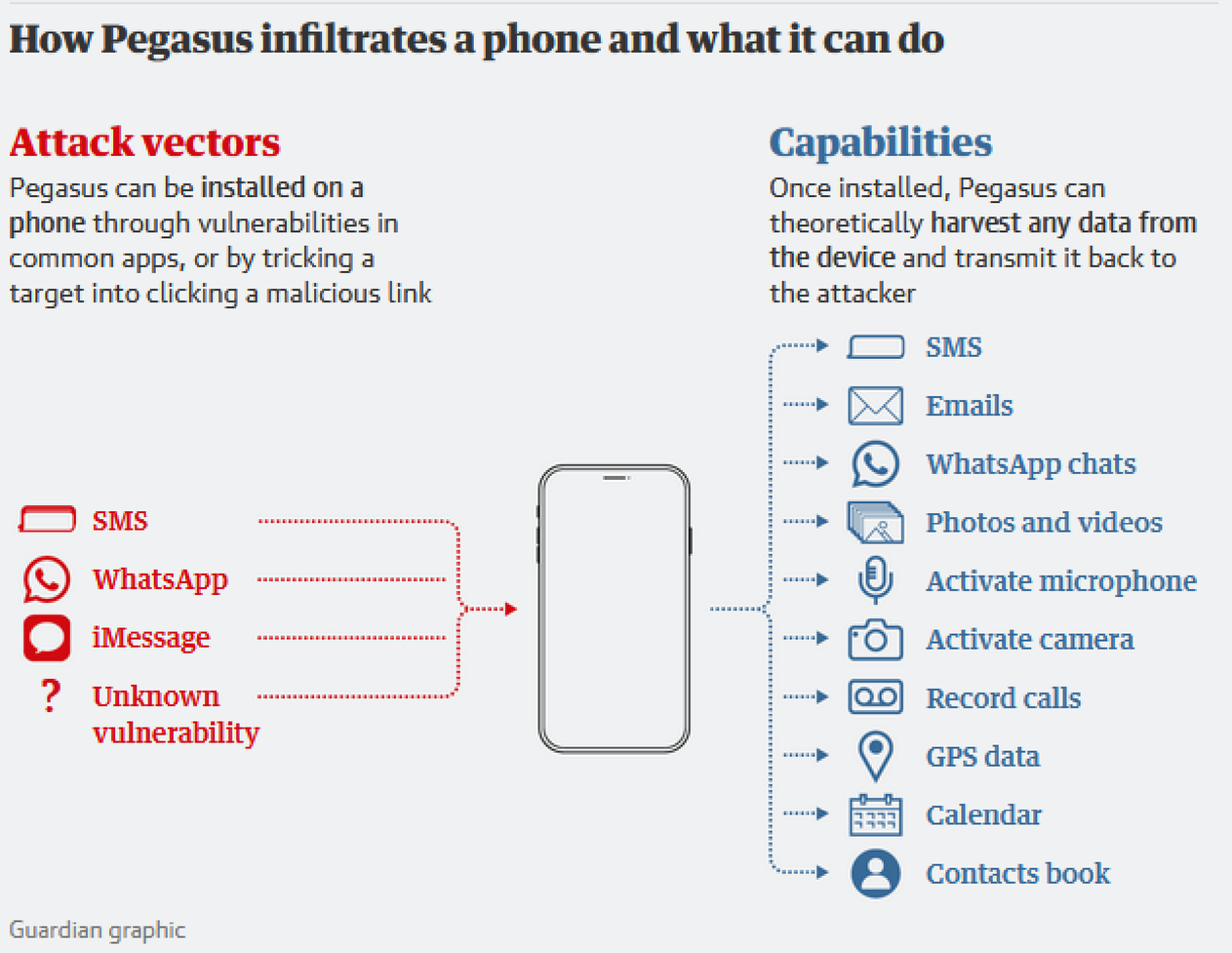
85 human rights activists

50,000 phone numbers leaked

Source: Pegasus Project

BBC

PEGASUS & PREDATOR

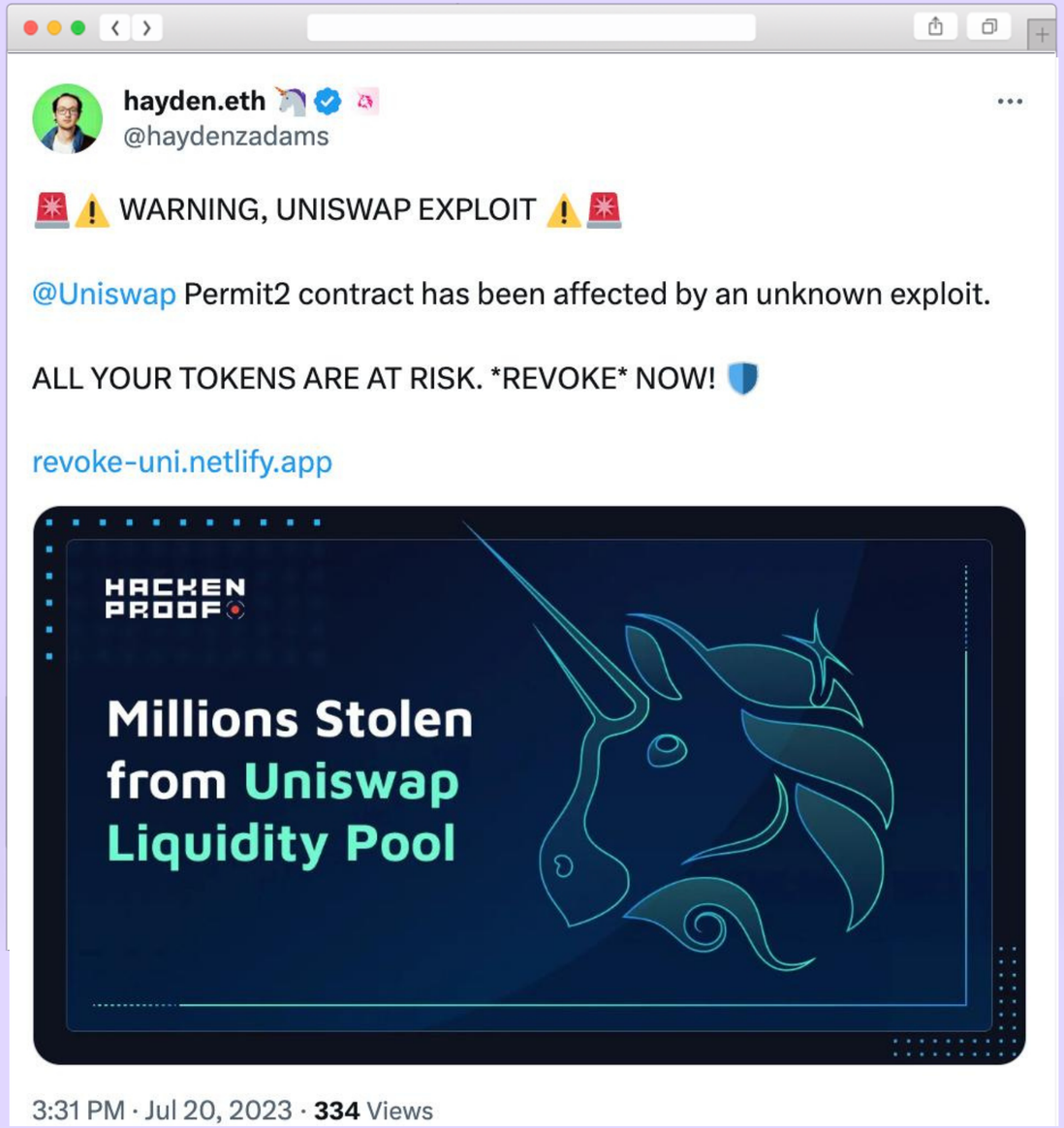


PEGASUS & PREDATOR

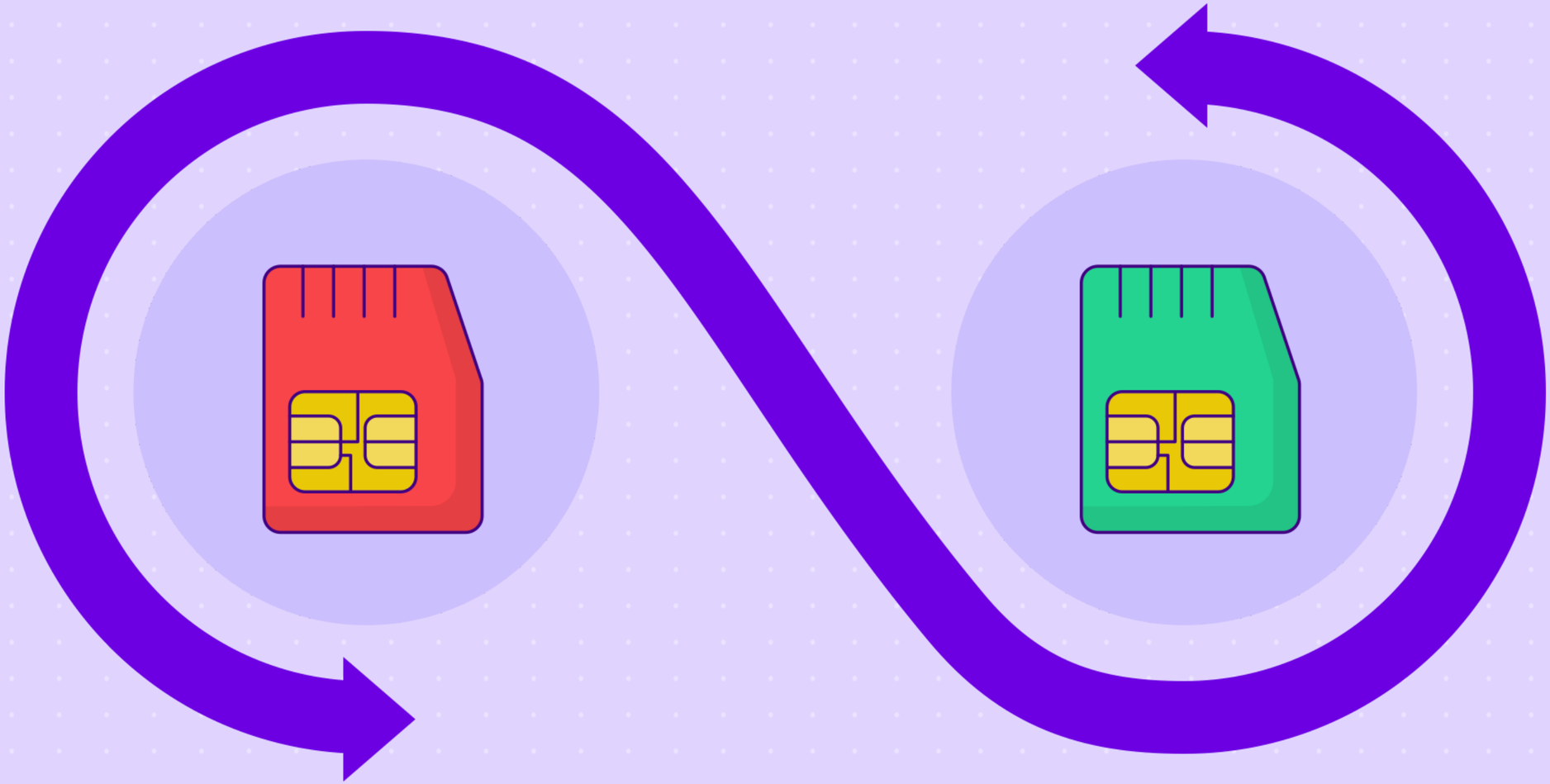
Hayden - Uniswap: Sim swap

defy EDUCATION

HAYDEN ADAMS



HAYDEN ADAMS



defy EDUCATION

Yuga Labs: Twitter hack

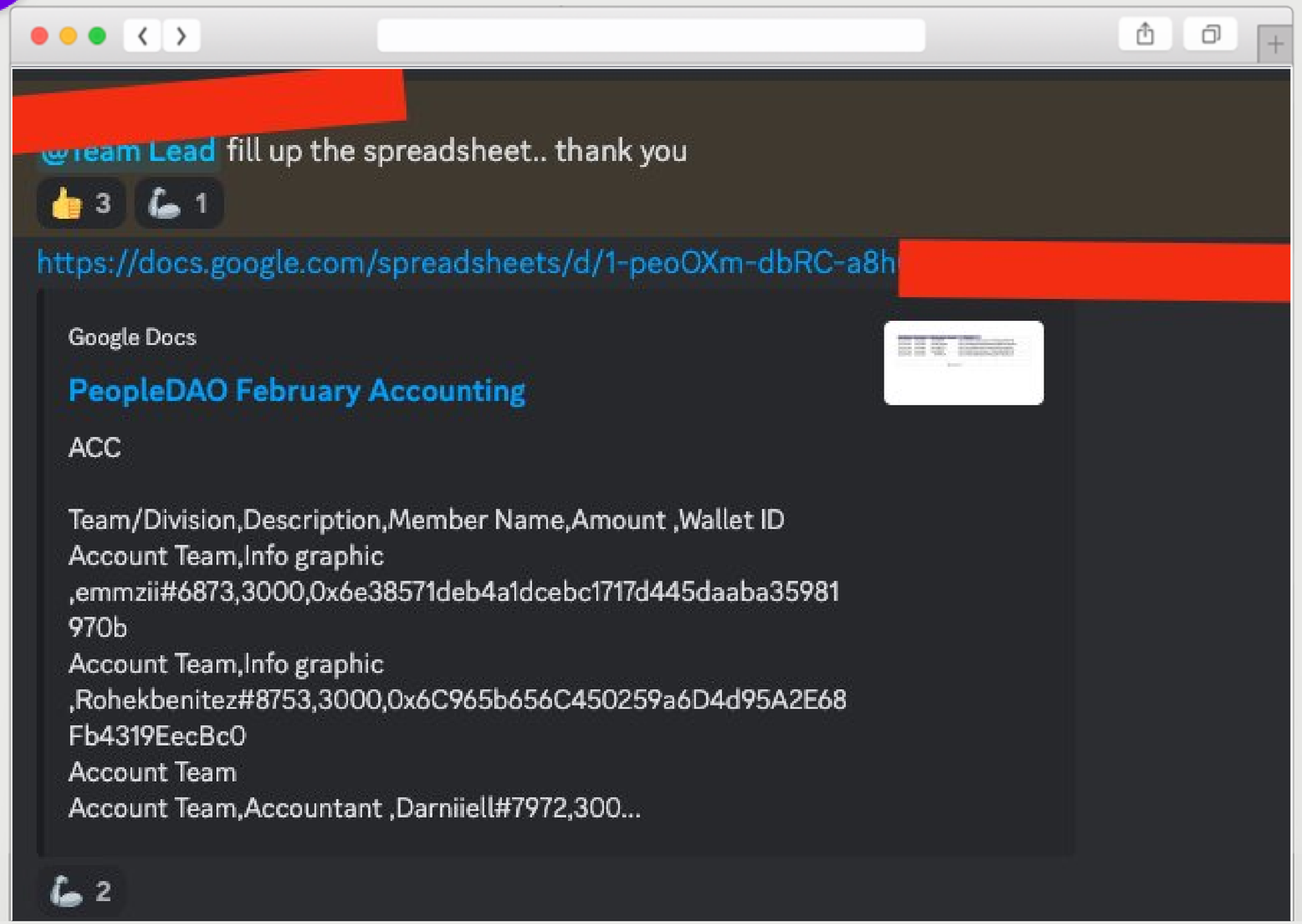
YUGA LABS


Daniel Alegre @dalegre · 2m
It's almost time to enter the Otherside. Start your journey at otherside.community before the portal closes!
Powered by @apecoin
otherside.community
12
14
375

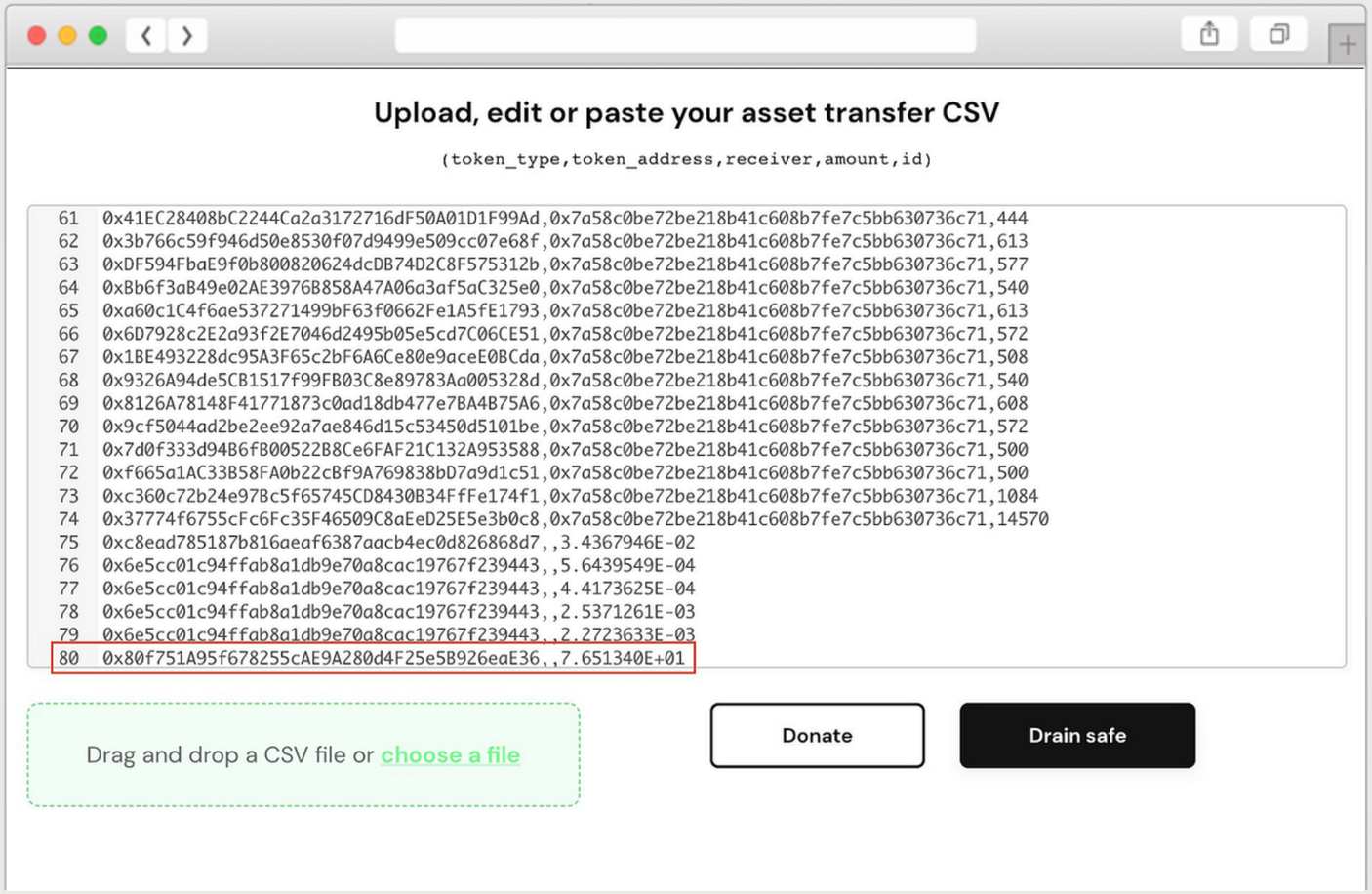
PeopleDAO: Google sheets edit

defy EDUCATION

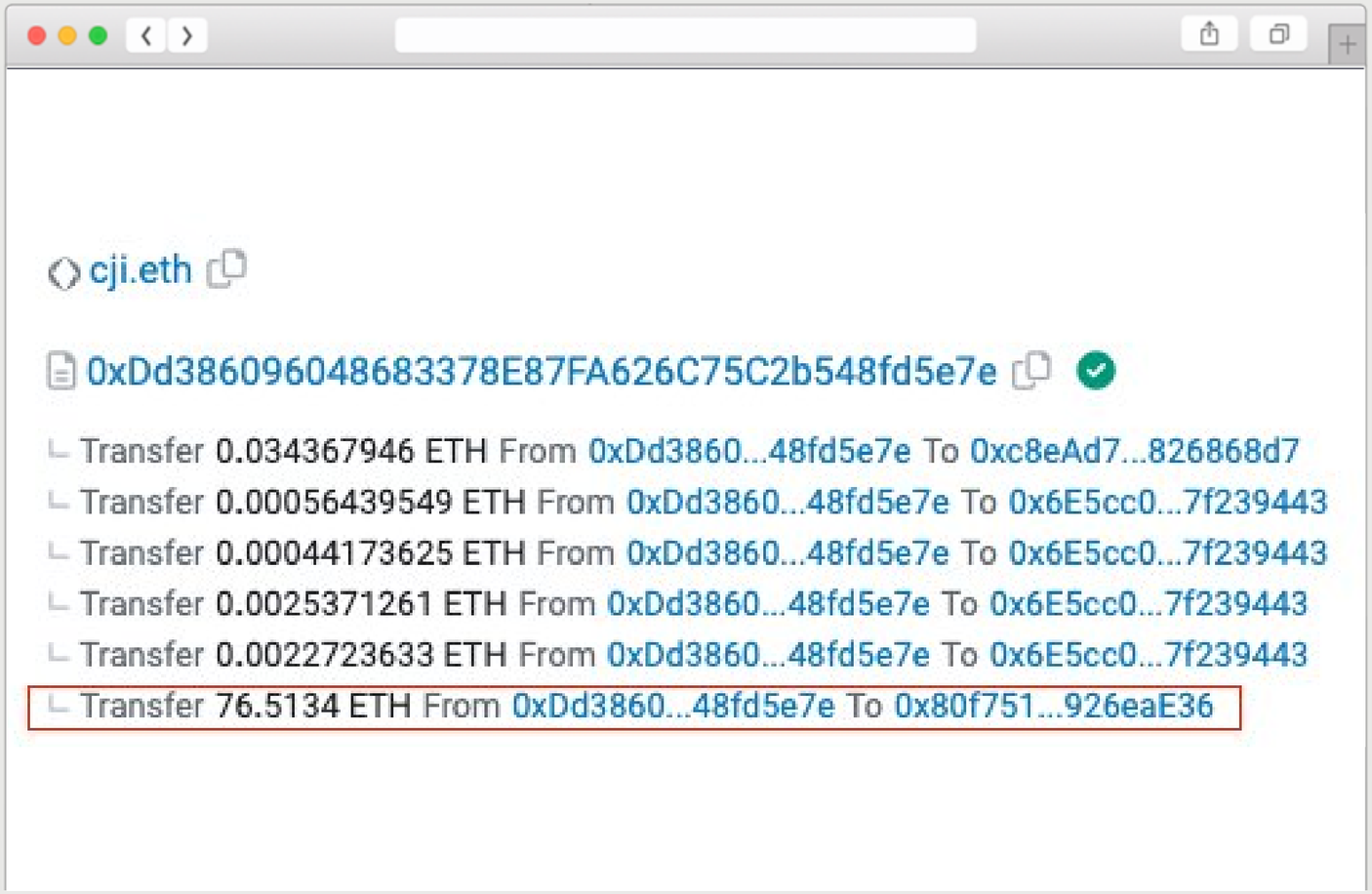
PEOPLE DAO


@Team Lead fill up the spreadsheet.. thank you
3
1
https://docs.google.com/spreadsheets/d/1-peoOXm-dbRC-a8h
Google Docs
PeopleDAO February Accounting
ACC
Team/Division,Description,Member Name,Amount ,Wallet ID
Account Team,Info graphic
,emmzii#6873,3000,0x6e38571deb4a1dcebc1717d445daaba35981
970b
Account Team,Info graphic
,Rohekbenitez#8753,3000,0x6C965b656C450259a6D4d95A2E68
Fb4319EecBc0
Account Team
Account Team,Accountant ,Darniiell#7972,300...
2

PEOPLE DAO


Upload, edit or paste your asset transfer CSV
(token_type,token_address,receiver,amount,id)
61 0x41EC28408bC2244Ca2a3172716dF50A01D1F99Ad,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,444
62 0x3b766c59f946d50e8530f07d9499e509cc07e68f,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,613
63 0xDF594FbaE9f0b800820624dcDB74D2C8F575312b,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,577
64 0xBb6f3aB49e02AE3976B858A47A06a3af5aC325e0,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,540
65 0xa60c1C4f6ae537271499bF63f0662Fe1A5fE1793,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,613
66 0x6D7928c2E2a93f2E7046d2495b05e5cd7C06CE51,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,572
67 0x1BE493228dc95A3F65c2bF6A6Ce80e9aceE0BCda,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,508
68 0x9326A94de5CB1517f99FB03C8e89783Aa005328d,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,540
69 0x8126A78148F41771873c0ad18db477e7BA4B75A6,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,608
70 0x9cf5044ad2be2ee92a7ae846d15c53450d5101be,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,572
71 0x7d0f333d94B6fB00522B8Ce6FAF21C132A953588,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,500
72 0xf665a1AC33B58FA0b22cBf9A769838bD7a9d1c51,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,500
73 0xc360c72b24e97Bc5f65745CD8430B34FfFe174f1,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,1084
74 0x37774f6755cFc6Fc35F46509C8aEeD25E5e3b0c8,0x7a58c0be72be218b41c608b7fe7c5bb630736c71,14570
75 0xc8ead785187b816aeaf6387aacb4ec0d826868d7,,3.4367946E-02
76 0x6e5cc01c94ffab8a1db9e70a8cac19767f239443,,5.6439549E-04
77 0x6e5cc01c94ffab8a1db9e70a8cac19767f239443,,4.4173625E-04
78 0x6e5cc01c94ffab8a1db9e70a8cac19767f239443,,2.5371261E-03
79 0x6e5cc01c94ffab8a1db9e70a8cac19767f239443,,2.2723633E-03
80 0x80f751A95f678255cAE9A280d4F25e5B926eaE36,,7.651340E+01
Drag and drop a CSV file or choose a file
Donate
Drain safe

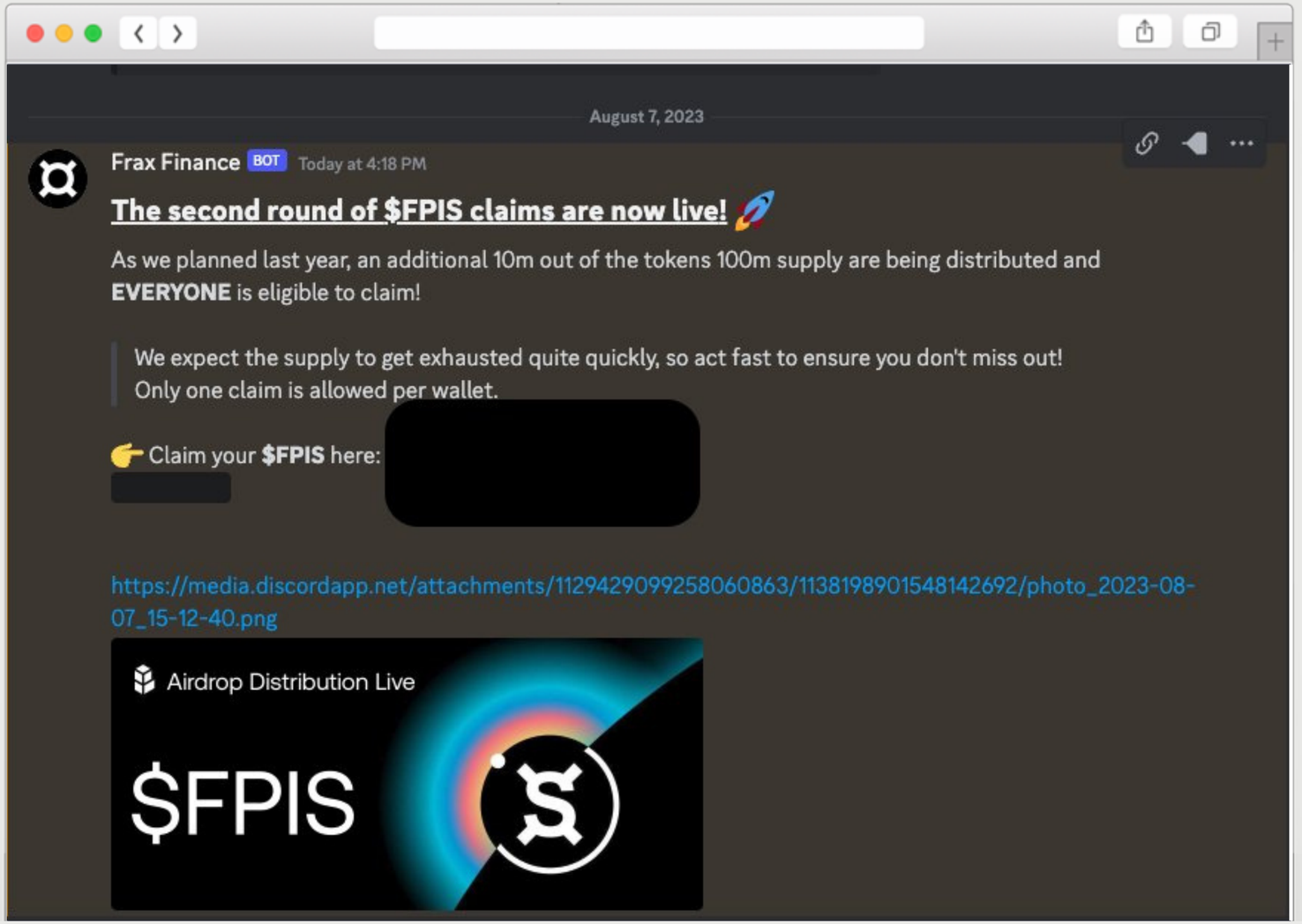
PEOPLE DAO



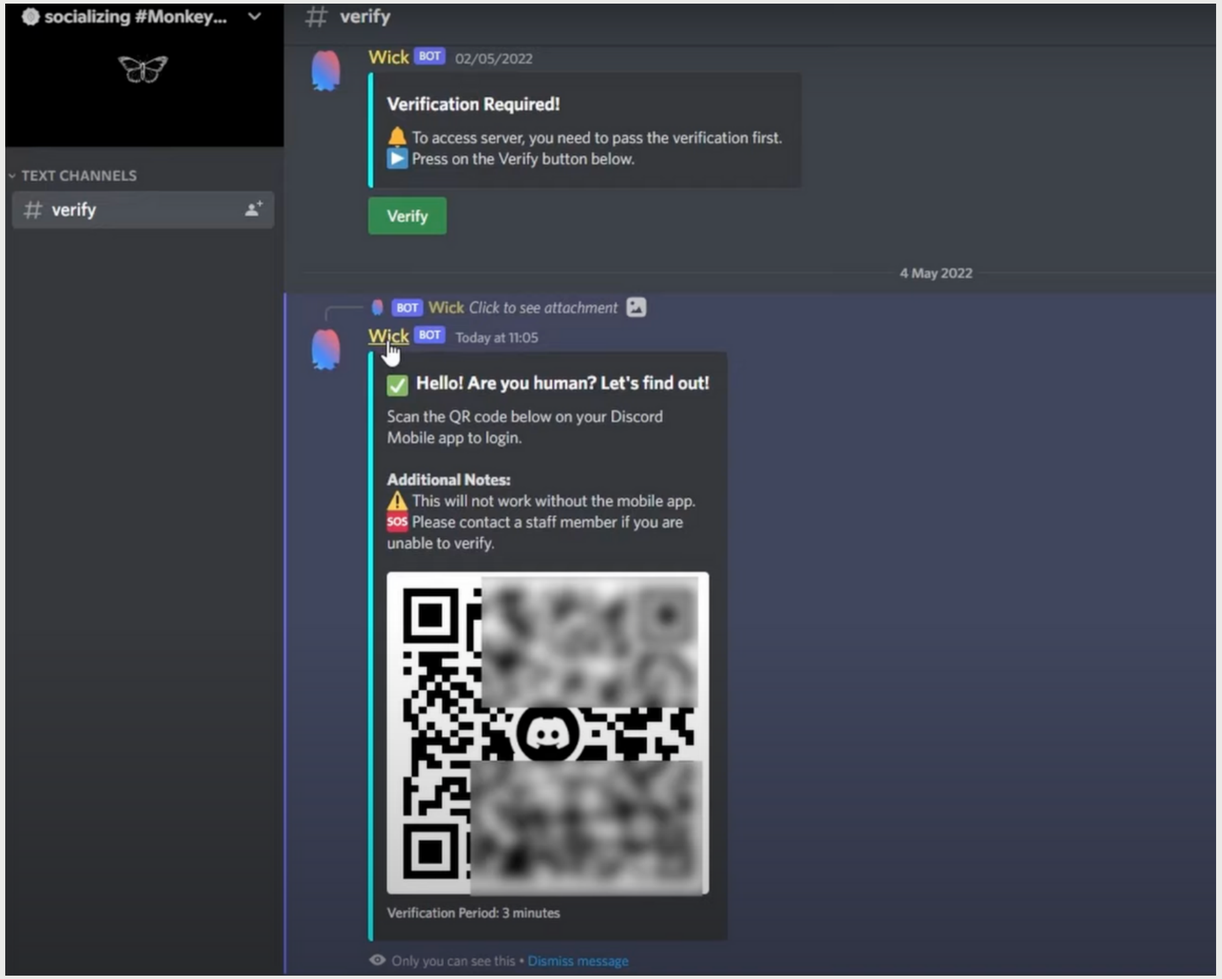
Frax Finance: Discord hack

defy EDUCATION

FRAX FINANCE

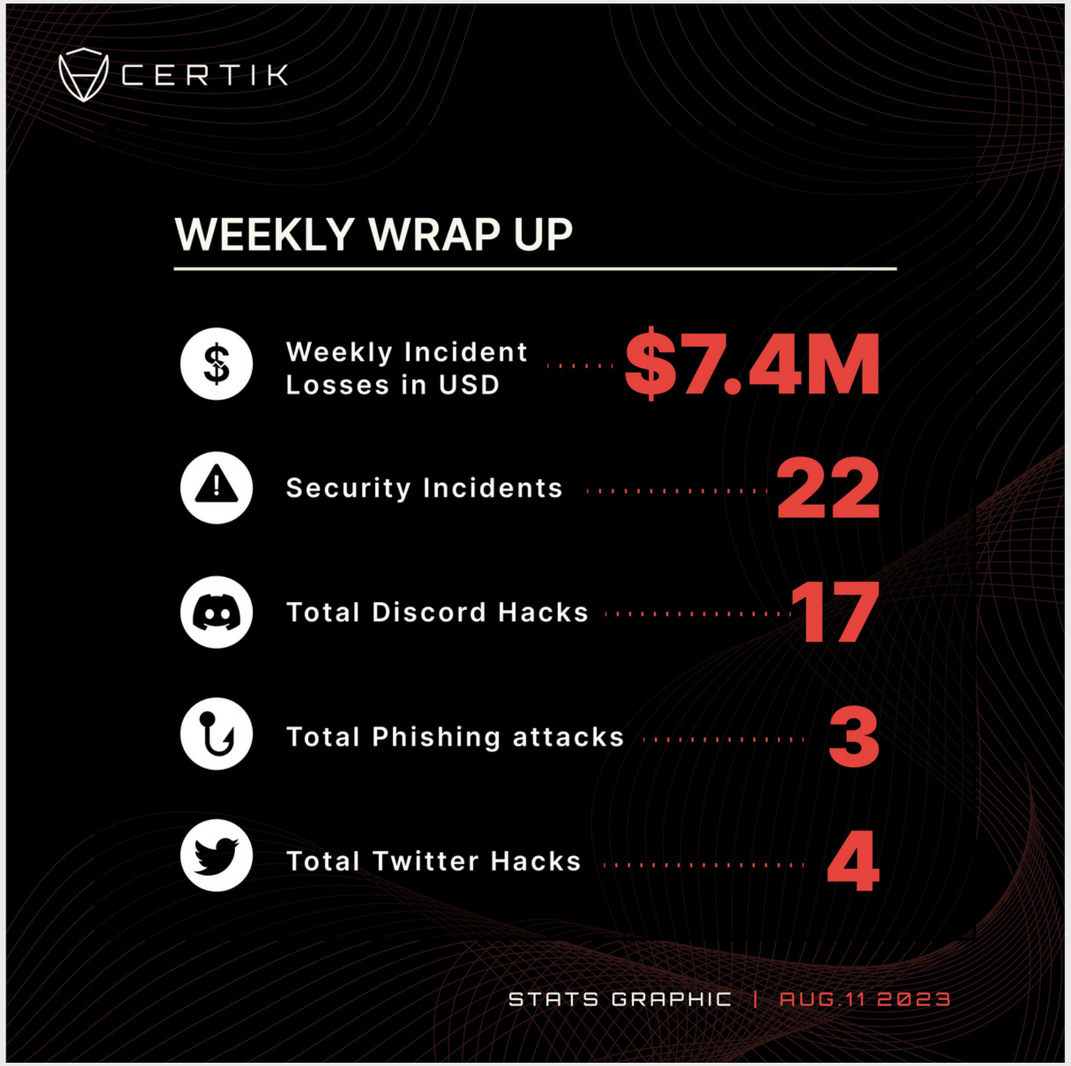


FRAX FINANCE



defy EDUCATION

FRAX FINANCE



defy EDUCATION

Rocketswap: Private keys

defy EDUCATION

ROCKET SWAP

Transaction Hash:	0xbe0b89188b044a3b69702c73fd76cf555b39fa4ad2d609685411b71cfa4f3dba
Status:	Success
Block:	17916284 815 Block Confirmations
Timestamp:	2 hrs 43 mins ago (Aug-14-2023 11:11:23 PM +UTC) | Confirmed within 2 secs
Transaction Action:	Supply 90,000,000,000,000 LoveRCKT And 400 Ether Liquidity To Uniswap V2
Sponsored:	
From:	0x96c0876F573e27636612CF306C9db072d2B13DE8
To:	0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D (Uniswap V2: Router 2) Transfer 400 ETH From Uniswap V2: Router 2 To Wrapped Ether
ERC-20 Tokens Transferred: 4	From 0x96c087...d2B13DE8 To Uniswap V2: LoveRCKT For 90,000,000,000,000 @loveloveroc... (LoveRC...) From Uniswap V2: Router 2 To Uniswap V2: LoveRCKT For 400 ($737,836.00) Wrapped Ethe... (WETH...) From Null: 0x000...000 To Null: 0x000...000 For 0.000000000000001 Uniswap V2... (UNI-V2...) From Null: 0x000...000 To 0x96c087...d2B13DE8 For 189,736,659.610102759919932612 Uniswap V2... (UNI-V2...)
Value:	400 ETH $737,836.00
Transaction Fee:	0.06200397158815714 ETH $114.37
Gas Price:	22.904077436 Gwei (0.000000022904077436 ETH)

defy EDUCATION

Casos de usuarios

CASO 1

Robo de bitcoins (2022)

- A un usuario le roban 16 bitcoins de su wallet self-custodial instalada en Windows
- La frase semilla había sido guardada de forma segura
- Usuario había descargado el Autocad crackeado de un sitio de torrents
- La laptop le comenzó a funcionar lento, por lo cual deshabilitó su antivirus
- El Autocad venía con un malware, el cual espera hasta encontrar una oportunidad
- El malware detectó la wallet instalada, robó el archivo de la private key y la envió
- El archivo fue desencriptado de forma remota y la billetera vaciada

MALWARE

defy EDUCATION

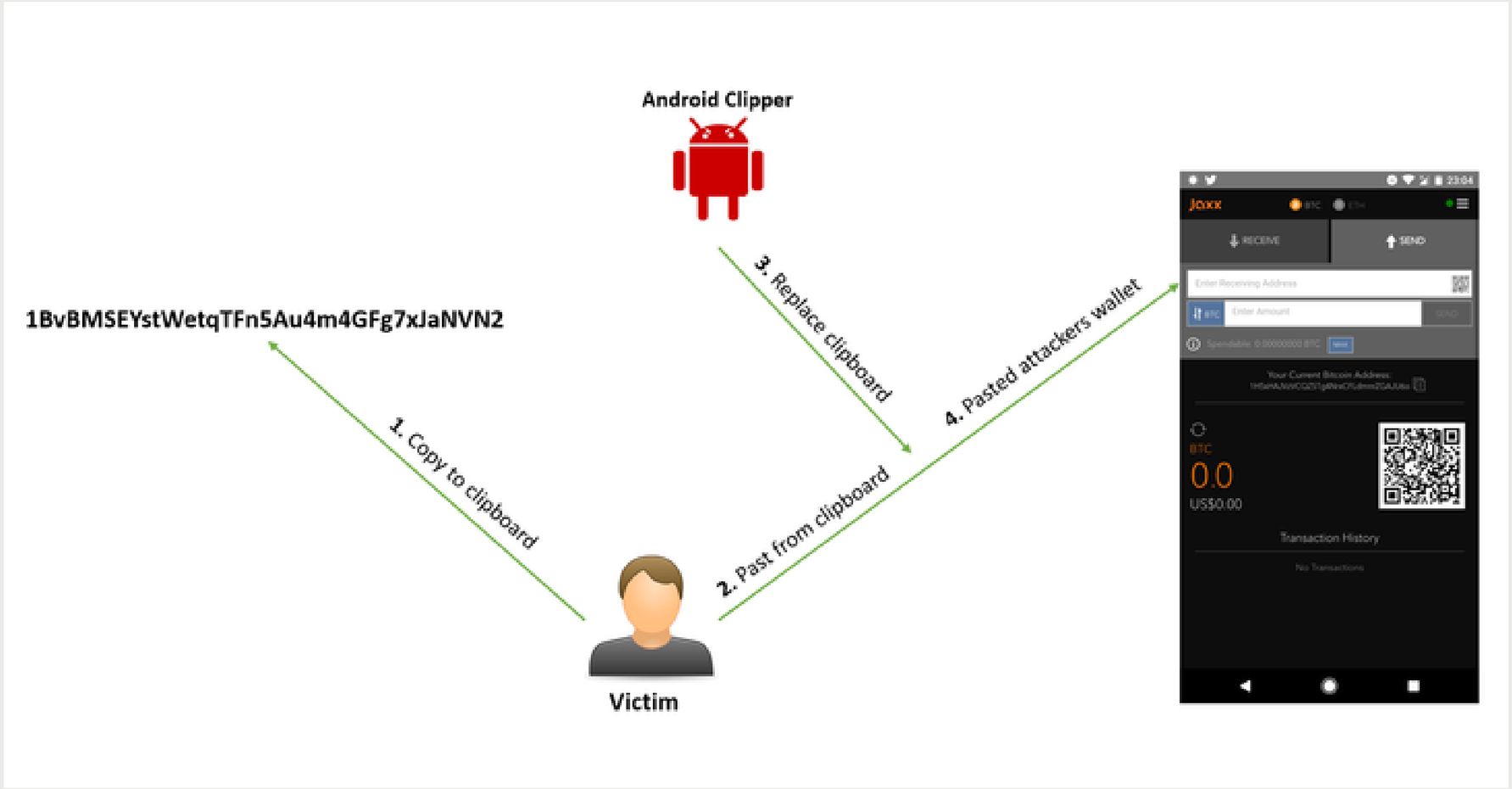
CASO 2

Robo de 25 ether

- Un usuario guarda sus tenencias en criptomonedas en una hardware wallet
- Envía 25 ether a otra de sus direcciones
- Los 25 ether son robados instantaneamente
- El usuario había descargado una aplicación con malware
- El malware monitorea el portapapeles de la computadora
- Cuando detecta que se copió una dirección de crypto, la reemplaza
- Los fondos son enviados a una dirección que no controlamos

defy EDUCATION

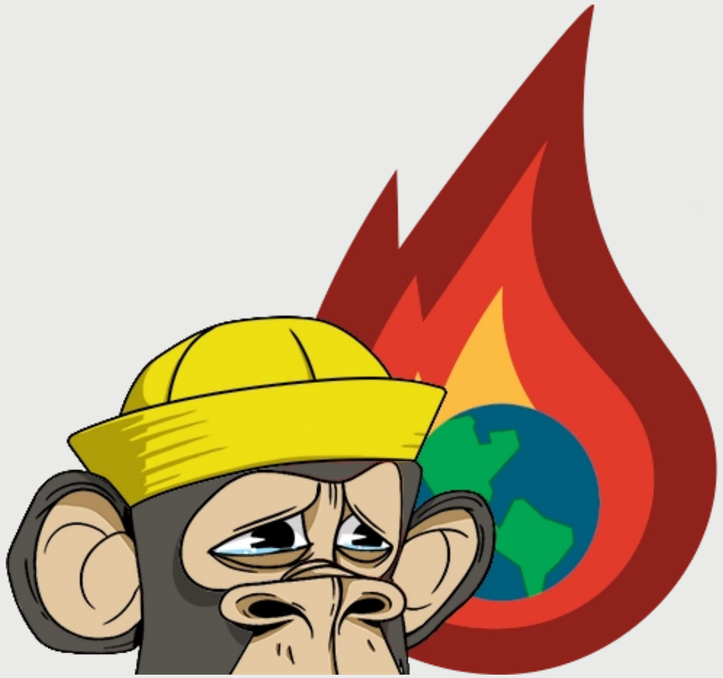
MALWARE


Android Clipper
1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2
3. Replace clipboard
1. Copy to clipboard
2. Past from clipboard
4. Pasted attackers wallet
Victim
Jaxx
RECEIVE
SEND
Enter Receiving Address
Enter Amount
BTC
0.0
US$0.00
Transaction History
No Transactions

FUENTES

rekt

rekt.news



web3isgoingjustgreat.com

defy EDUCATION

MUCHAS GRACIAS!

defy EDUCATION