



black hat[®]
USA 2024

AUGUST 7-8, 2024
BRIEFINGS

From Doxing to Doorstep:

Exposing Privacy Intrusion Techniques used by Hackers for Extortion

Jacob Larsen

whoami



  @larsencyber

<https://larsencyber.com>

Jacob Larsen

- Offensive Security Team Lead @ CyberCX
- Threat Researcher
- Researching underground cyber crime groups since 2016
- Based in Perth, Australia

[NAME]

FIRST Name: Jacob

LAST NAME: Larsen

USERNAMES: " [REDACTED] ", " [REDACTED] ", " [REDACTED] ", " [REDACTED] "
" [REDACTED] ", " [REDACTED] ", " [REDACTED] ",

- 9 years ago, I was a doxing victim.
- I had an online account with a rare username which they wanted.
- Ever since then, I have followed the subculture surrounding doxing and those participating.

[ADDRESS]

STREET: [REDACTED]

STATE/CITY: [REDACTED]

COUNTRY: Australia

POSTAL CODE: [REDACTED]

TIMEZONE: AWST

ViLE: Breaching a DEA Data Portal



PRESS RELEASE

**Two Men Charged for Breaching
Federal Law Enforcement Database
and Posing as Police Officers to
Defraud Social Media Companies**

Tuesday, March 14, 2023

<https://www.justice.gov/usao-edny/pr/two-men-charged-breaching-federal-law-enforcement-database-and-posing-police-officers>

- In March 2023, 2 members of a notorious doxing gang “ViLE” were charged for breaching a Drug Enforcement Agency data portal.
- This portal allowed them to search for anyone’s personal information across 16 different federal law enforcement databases.

View/Edit Request 648889

Police Offices



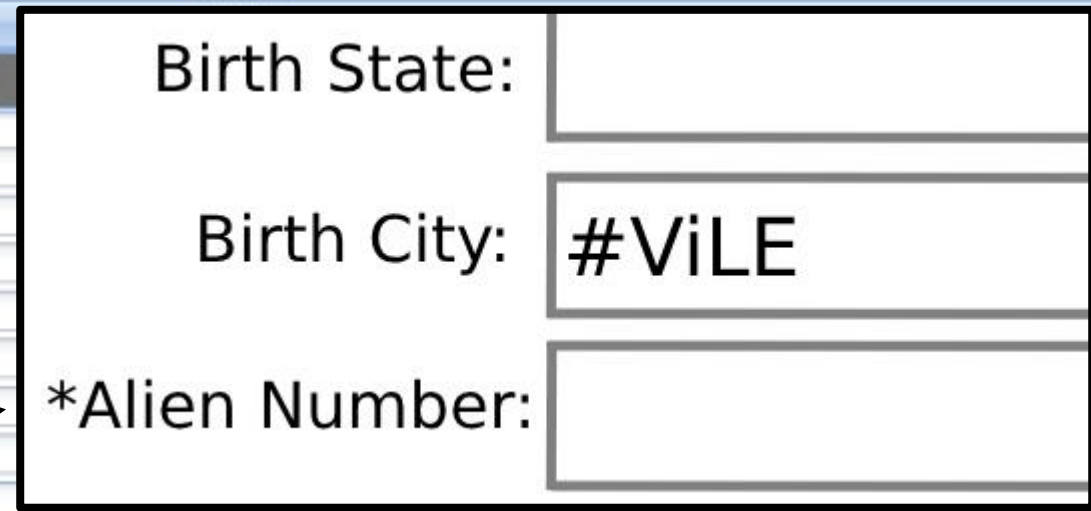
ID: 648889
 Request Status: WORKING
 Created Date: 04/09/2022
 Created By: [Redacted]
 Last Modified Date: 05/08/2022
 Last Modified By: [Redacted]
 Assigned To: [Redacted]

Activity Type: [Redacted]
 Deconfliction: NO

Remarks

Address Aircraft Business DOT Drone **Person** Phone Vehicle Vessel Weapon

*Last Name: BRIAN
 Maternal Name:
 *First Name: KREBS
 Middle Name:
 *DOB:
 Birth Country:
 Birth State:
 Birth City: #VLE
 *Alien Number:
 Gang(DTO)/Cartel (suspected):



Systems

Basic

- LEIA
- EPIC10
- ELISA
- EID
- DPO
- NSS
- PRIVILEGE

Select All

#ViLE

7. Once they have obtained a victim's information, SENOH and CERACOLO post the information in an online forum, hereinafter referred to as Forum-1, that is administered by the leader of VILE ("CC-1"). Victims are extorted into paying CC-1 to have their information removed from Forum-1. SENOH also uses the threat of revealing personal information to extort victims into giving him access to their social media accounts, which SENOH then reveals.

ViLE: Doxing for Extortion

- ViLE used this access for “doxing”, which is slang for “dropping documents”, also known as dropping information which links someone’s public identity with their online username.
- The intention of doxing is to intimidate victims and make them fearful of “what might happen” when their personal information is uploaded on a website where it won’t be taken down.
- This is why adversaries choose to use websites like **Doxbin**.



[Official Doxbin Telegram](#)

[Mirrors: doxbin.org | doxbin.com | doxbin.net](#)

Search for a paste

Showing 150 (of 133419 total) pastes

« 1 2 3 4 5 ... 890 »

Pinned Pastes

| Title | Comments | Views | Created by | Added |
|---|----------|--------|--|----------------|
| Development Changelog | - | 33727 | Reiko [Council] | Sep 7th, 2023 |
| How to Ensure Your Paste Stays Up | - | 179812 | Operator [Admin] | Nov 20th, 2020 |
| Transparency Report | - | 138370 | Operator [Admin] | Jun 20th, 2020 |

Doxbin

- Doxbin is a doxing website that offers adversaries, or their users, a place to upload doxes where they won't be taken down. As per their website it says:

“if your information goes up, it won't come down unless it breaks our terms of service”

- A feature Doxbin offers upgraded users is the ability to publish private doxes.

Doxbin Account Upgrades

| | |
|--|-------------------------|
| Rich | \$100 |
| PERKS | |
| Username preview | Anonymous [Rich] |
| Name color | Sparkling gold |
| Paste highlight color | Gold |
| More noticeable | ✓ |
| .GIF profile picture | ✓ |
| Instant paste edits | ✓ |
| Unlist your own pastes | ✓ |
| Private your own pastes | ✓ |
| Password protected pastes | ✓ |
| Username changes | 3 |
| Purchase with Bitcoin or Monero | |



| ID | Username | Comments | Pastes | Join date |
|--------|-----------------------|----------|--------|------------|
| 294260 | Joana | 157 | 1941 | 1 year ago |

| Information | |
|----------------|------------|
| User ID | 294260 |
| Joined | 1 year ago |
| Pastes | 302 |
| Comments | 174 |
| Following | 0 |
| Followers | 73 |
| Likes Given | 2 |
| Likes Received | 309 |

$$1941 - 302 = 1639 \text{ "Private" Doxes}$$

Doxbin

- This means adversaries can upload a victims dox, and then send them a private link to it on Doxbin.
- Next, the adversary will attempt to extort the victim by threatening to release their personal information publicly and to the Doxbin community.
- Due to this simple functionality, Doxbin has become the largest doxing community online and amassed 300,000 users and over 165,000 published doxes.

Doxbin Admins

ViLe Members

brenton



kt



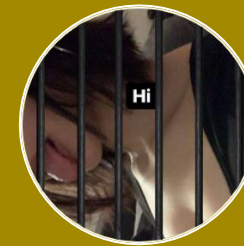
ego



cain



weep



convict



Doxbin & ViLE

- Doxbin was founded in 2018 by two actors, called “Kt” and “Brenton”.
- “Kt” is one of 5 members of the doxing gang “ViLE”. The other members are “Ego”, “Cain”, “Weep” and “Convict”.
- “Weep and “Convict” were the members charged by authorities, with the remaining members wanted for their involvement.
- To get better insights into the doxing techniques they used, I personally conducted an interview with “Ego”, a member of ViLE that wasn’t apprehended.

Doxbin Admins

ViLe Members

brenton



kt



ego



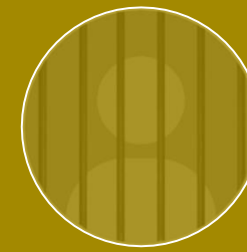
cain



weep



convict



who is *Ego*?

Started out in XBOX Live ISP Doxing scene.

Member of wanted gang "ViLE".

Doxed key LAPSUS\$ member "white".

Earns \$100k+ from doxing and extortion.

Schizophrenic and emotionally detached.



ego

Do you ever use private sources to enrich your data for doxes?



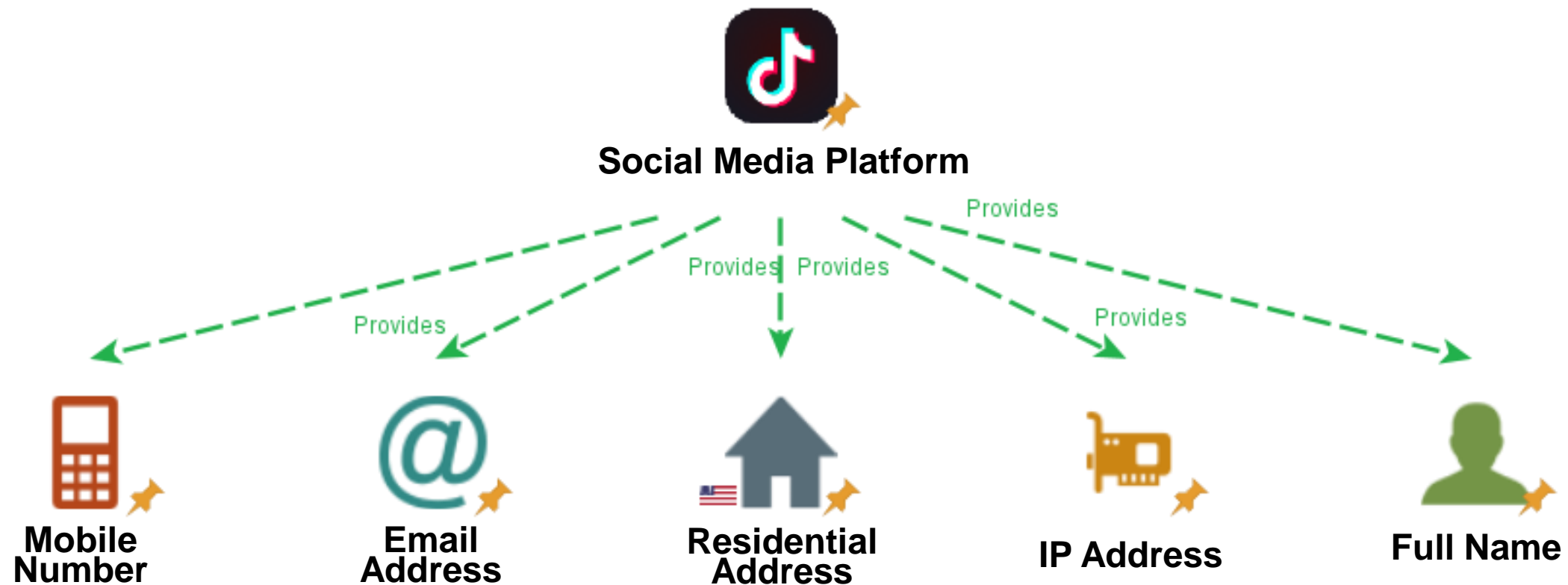
ego

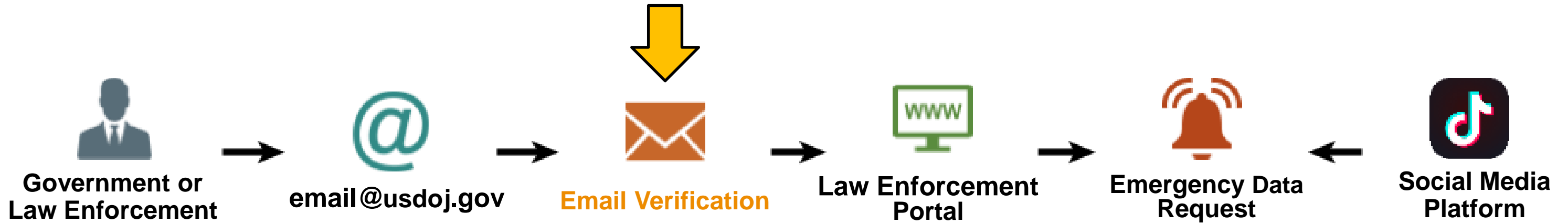
Yes, nearly every time.
I've taught loads of people to do the same.

- Private databases,
- TLO lookups,
- Social engineering customer service,
- Insiders at mobile carriers, and
- Fraudulent Emergency Data Requests to social media companies.

What is an Emergency Data Request?

- A procedure used by law enforcement in **emergency situations**.
- Information provided by service providers in less than 24 hours.
- **Circumvents** the need for a **subpoena**, due to an **immediate threat**.





To access our Law Enforcement Online Request system click:

https://www.facebook.com/records/login/auth/?token=MDXqhytshHrS8sZDC09K0ddhuKGD-QKY-_M-c4vzPFIEJHDTwEuQIC-zZGAwmEEUqkhyV7mKuw993k2AB0y0HZnFPkNUU57nFB0x5

Thank you,
Law Enforcement Response Team

Emergency Data Requests (EDR)

- Before an Emergency Data Request can be submitted, an identity verification process is required.
- For most Law Enforcement panels, this simply requires a Government email address to receive an authorization link, as shown in the previous slide.
- There are also aggregator platforms which offer Government workers a single portal to lodge multiple requests, against a variety of service providers simultaneously, as shown in the next slide.

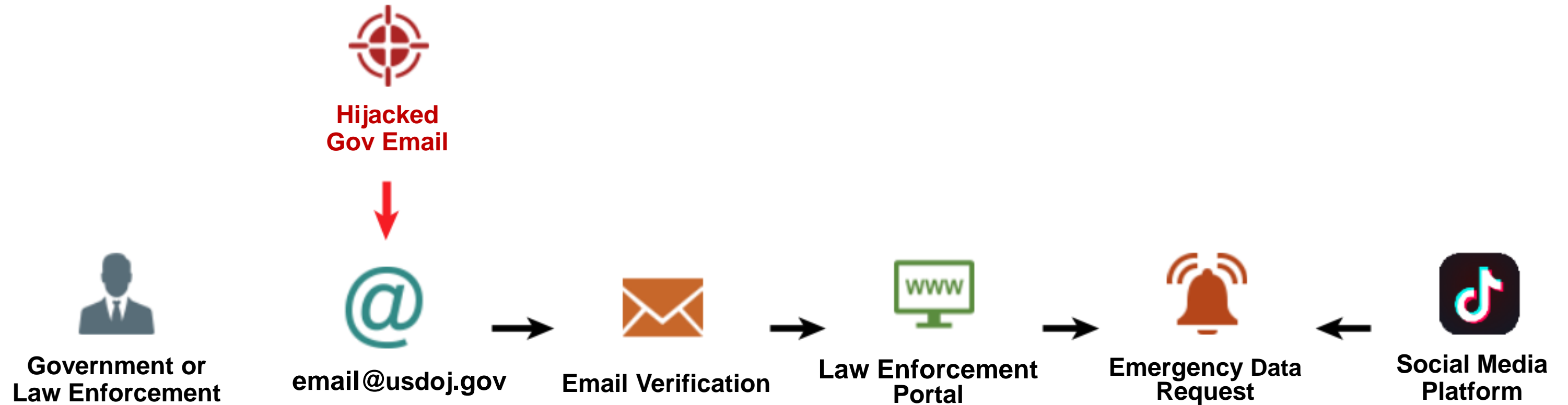
The screenshot displays a web application interface with a dark sidebar on the left and a main content area with a grid of logos. The sidebar contains the following navigation items: Profile, Notifications, Requests, Home, New Request, Proactive Reports, and Proactive Reports. The main content area features a grid of logos for various companies, including Amino, Authy, Badoo, BIMeta, BINANCE, bumble, Chainlink, Coinbase (INTL and US Law Enforcement), Cross River, Discord Government Information Request, Fidelity, FRUITZ, gab, Hack/House, Hinge, imgur, kik, KR, LinkedIn, Match Group, MoonPay, and official.

| | | | | | |
|-----------|---|--------------------------------|--------------|---|----------|
| Amino | Authy | BADOO | BIMeta | BINANCE | bumble |
| Chainlink | coinbase INTL Law Enforcement Click to request access | coinbase US Law Enforcement | cross river | Discord Government Information Request | |
| Fidelity | FRUITZ | gab | «Hack/House» | Hinge | imgur |
| kik | KR | Linkedin | Match Group | MoonPay | official |

Fraudulent Emergency Data Request

- Given the depth of information service providers have on users...
- If a **fraudulent** Emergency Data Request could be completed, it would be the **fastest** and **most efficient** way for an adversary to obtain **highly accurate** and **sensitive** data on a victim.
- Submitting a **fraudulent** request, only requires access to compromised Government email address, as this allows the adversary to verify themselves on Law Enforcement panels by receiving the authorization link.

Fraudulent Emergency Data Request



Fraudulent Emergency Data Request

- Government emails can be easily purchased on underground forums and Telegram communities, for the cheap price of \$70 USD.
- They are typically obtained from information stealer malware logs, hijacked cPanels, and phishing.
- I went undercover and infiltrated invite-only communities where threat actors both sell Government emails and provide the service to submit fraudulent Emergency Data Requests.

Government Email Access

- Government Email Access
- Government Panels Access
- Occasionally, Gov IDs

All for \$70 each
Our mails can be used for

\$70 each

Law Enforcement Portals

- Law Enforcement Portals

- Any other "Law Enforcement" or "Government Only" Services

You can view our current stock [Here](#)
Our stock list updates every few days. Don't see what you need?
Check again later, it probably be there.
If you'd like to purchase, please contact me @

The screenshot shows the cPanel interface. On the left sidebar, the 'Email Accounts' tool is highlighted with a red box and a red arrow. The main content area displays a list of government email domains under the heading 'Gov Emails Custom Gov Emails'. A dark overlay box contains the following text:

```
Gov Emails  
Custom Gov Emails  
.gov.mz *Mozambique /direct * 🇲🇵  
.gov.ph *Philippines /direct * 🇵🇭  
.gov.pk *Pakistan / direct * 🇵🇰  
.gov.br *Brazil / subdomain* 🇧🇷
```

Below the list, it states: 'Direct domain - 125 USD' and 'Subdomain - 100 USD'. A red arrow points to the text: 'You can use them for phishings, EDR's, leads, scams, etc...'. On the right side of the interface, a 'General Information' panel is visible, showing details for the current user, including the primary domain, shared IP address, home directory, and last login IP address.

email accounts

- Email
- Email Accounts**
- Autoresponders
- Track Delivery
- Email Deliverability
- Encryption
- Email Disk Usage

Gov Emails
Custom Gov Emails
.gov.mz *Mozambique /direct * 🇲🇵
.gov.ph *Philippines /direct * 🇵🇭
.gov.pk *Pakistan / direct * 🇵🇰
.gov.br *Brazil / subdomain* 🇧🇷

Direct domain - 125 USD
Subdomain - 100 USD

You can use them for phishings, EDR's, leads, scams, etc...

General Information

Current User
[redacted]@gov

Primary Domain
*****.gov.mz

Shared IP Address
[redacted]

Home Directory
/home/[redacted]@gov

Last Login IP Address
[redacted]

n***l@usdoj.gov



safety-enforcement.tiktok.com/ticket_type=1

TikTok safety enforcement tool

Law enforcement requests

- Submitted
- Under review
- More info needed
- Closed

n***l@usdoj.gov

+ New request

https://safety-enforcement.tiktok.com/ticket_type=1

TikTok safety enforcement tool

Law enforcement requests

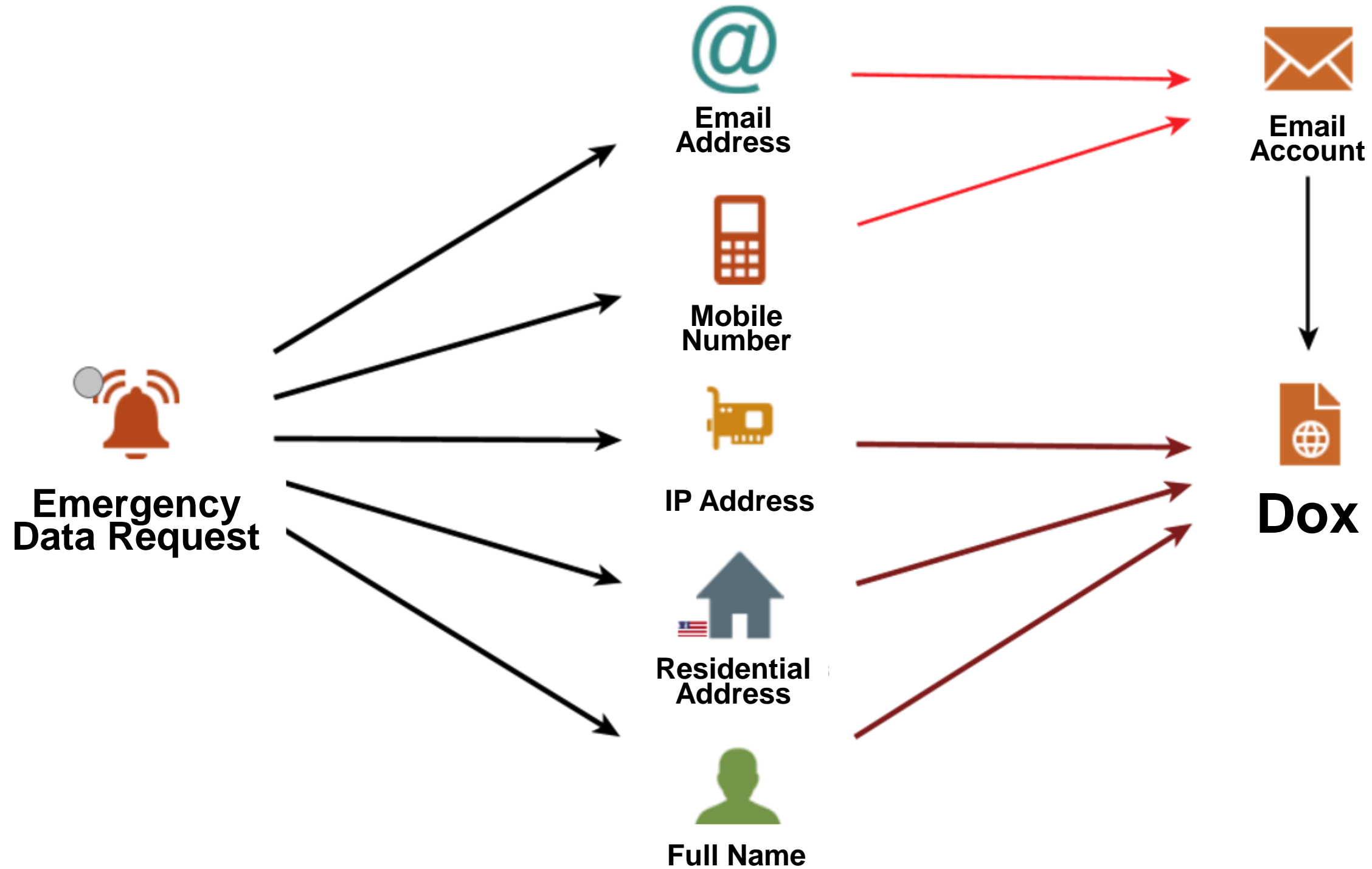
| Reference number | Creation date |
|------------------|---------------|
| Ref number | |

I have 2x US top tier 2:07 PM

@fbi.gov and @usdoj.gov 2:07 PM

Fraudulent Emergency Data Request

- Once a fraudulent Emergency Data Request is completed the adversary will attempt to **compromise the victim's personal accounts**, to get other sensitive information they can add to the victim's Dox.
- Historically simply the fear of “what might happen” when a victim's personal information was released online, was enough for them to meet extortion demands.



Violence-as-a-Service

- This was because adversaries had no way to intimidate their victims in real life, and it was just seen as a virtual threat.
- However, due to new “Violence-as-a-Service” marketplaces, digital conflicts now manifest physically, with real life consequences.
- In my interview with “Ego”, I asked if Doxbin members pay for their targets to be intimidated physically, and he shared that even some of the members provide these services.

Do Doxbin members pay for their targets to be bricked or intimidated physically?



ego

Those who have the means often go for it, and some of the members even provide these services.

The range of offerings is quite extensive, from bricking, to firing shots at their homes from the outside.

These acts are usually driven by the motive to acquire cryptocurrency.

Listen to
hear...



*“ViLe has
come to get
yah!”*

#ViLe

Violence-as-a-Service

Harassment

- Swats (USA & CA + UK + EU) ~50\$ 30\$
- Constant calling, trolling, messaging (ANY COUNTRY) ~ 25\$
- Get anyone jumped (UK + EU + USA) ~ 170\$
- Get any house bricked (USA + UK+ EU) ~ 285\$ 200\$
- Get your target stabbed (UK + USA) ~ 12,000\$
- Get your target kidnapped (UK) ~ 24,500\$

^

Comes with video proof for any of these

 MM / Escrow Accepted

 24/7 Online

Contact me: 

Channel: 





ego

There's those who take it a step further, and break into the residence, torturing these individuals with anything from

cutting their fingers off to killing them, all to take the crypto currencies they behold.

Things get pretty wicked online, much more than people realize.

PRESS RELEASE

Man Convicted of Violent Home Invasion Robberies to Steal Cryptocurrency

9. The Husband described Perpetrator-2 as very threatening. Perpetrator-2 threatened to cut off Husband's toes and genitalia, to shoot him, and to rape his wife if he didn't access his Coinbase account. Perpetrator-2 also struck the husband in the head. The Husband reported that

Violence-as-a-Service

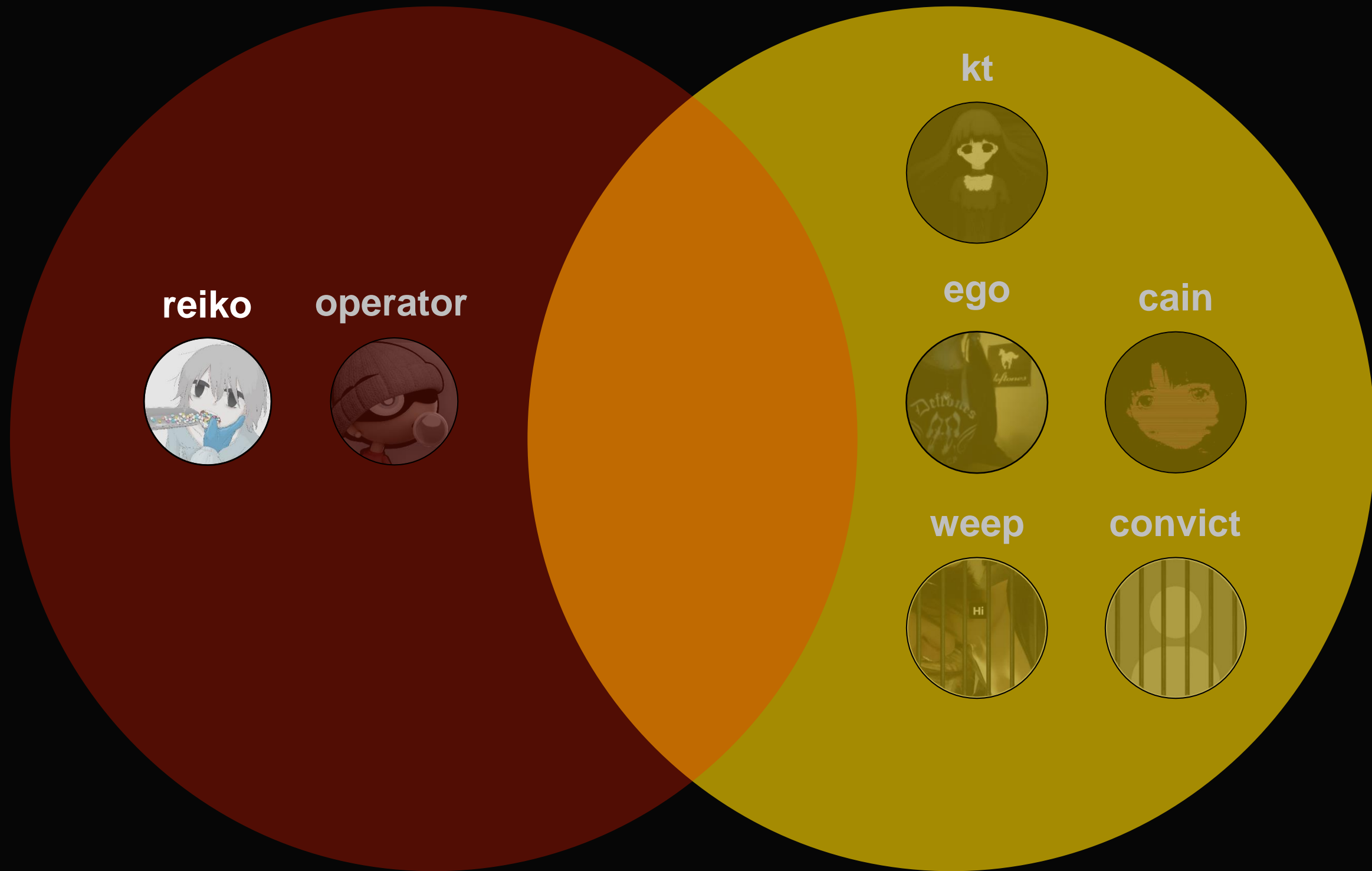
- Cutting off someone's fingers is quite different to throwing a brick through their window, however it is happening, and recent arrests prove this.
- In June 2024, a Florida man was convicted of doxing and extorting victims for their cryptocurrency, just like "Ego" said in the interview.
- He broke into victim's homes, and took them hostage, even threatening to cut off their fingers and toes.
- This brings to life the doxing and extortion tactics used by gangs like ViLE.

Doxbin & ViLE

- ViLE disbanded within months of “Weep” and “Convict” being charged.
- “Kt” also went into hiding and decided to part ways with Doxbin.
- Doxbin was sold to “Operator” in June 2023, and “Reiko” stepped in as a new system administrator and developer.
- With an interest in wanting to better understanding the legality of Doxbin, I was able to organize an interview with “Reiko” to shed some light.

Doxbin Admins

ViLe Members



reiko



operator



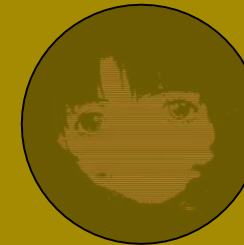
kt



ego



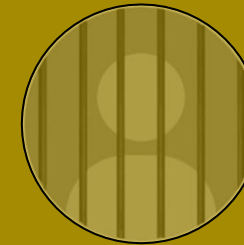
cain



weep



convict



who is *Reiko*?

Started Doxing in 2016 when he was a minor.

Involved in SWAT'ing attacks on women.

Leader of doxing gang called "Valhalla".

Developer and system administrator of Doxbin.



reiko

How do you ensure operational security with Doxbin infrastructure?

Do you rely on bulletproof hosting?



Bulletproof hosting is not necessary.

Doxbin is not illegal.
This is due to Section 230 of the
Communications Decency Act

Offshore.CAT is a Doxbin Project.



Legality of Doxbin

- In the interview “Reiko” shared that “*bulletproof hosting is not necessary*” because “*Doxbin is not illegal*”.
- However, this didn’t seem to be correct, as Doxbin runs a service called “offshore.cat” which recommends offshore hosting providers.
- The website includes reviews that specifically mention Doxbin’s experiences.
- It’s clear that offshore hosting providers are used by Doxbin operates in a legal gray area.

The Real Offshore Hosting List

OFFSHORE.CAT

The Real Offshore Hosting List

 **HOSTINGS**

 **DOMAINS**

 **VPN**

 **EMAILS**

 **CDN/WAF**



About

Offshore.CAT is a compiled list of the real & genuine, along with the bad & garbage offshore services that we have either used/have had experience with in the past.

We publish these reports because I'm tired of getting asked what hosting they should use. Offshore.CAT is not affiliated with any of the listed websites, our website takes zero responsibility from legal or unethical usage.

All informations are exposed as is and might be not up to date if something recently changed.

Offshore.CAT is a [Doxbin](#) Project.

Updated 2023-08-04

Total sites 71







About


Offshore.CAT is a compiled list of the real & genuine, along with the bad & garbage offshore services that we have either used/have had experience with in the past.

We publish these reports because I'm tired of getting asked what hosting they should use. Offshore.CAT is not affiliated with any of the listed websites, our website takes zero responsibility from legal or unethical usage.

All informations are exposed as is and might be not up to date if something recently changed.

Offshore.CAT is a [Doxbin](#) Project.

| Name | Website link | Description | Company country | Log policy* |
|--------------------------|---------------------------------------|--|---|-----------------------------|
| Hostings | hostings.offshore.cat | A 24/7 web log for support & updates |  | Requires email confirmation |
| Domains | domains.offshore.cat | Used by the infamous Pornopolitics |  | Requires email confirmation |
| Emails | emails.offshore.cat | Owned by "Wanted" Carbone, current administrator of "Doxbin" email service |  | Requires email confirmation |
| VPN | vpn.offshore.cat | A real offshore hosting that doesn't ask for many questions |  | Requires email confirmation |
| CDN/WAF | cdnwaf.offshore.cat | Helped protect The Tea Project in 2019, Doxbin certified |  | Requires email confirmation |
| CDN/WAF | cdnwaf.offshore.cat | Great owner who helped a friend out of a |  | Requires email |

[Namecheap](#) [Namecheap](#) An extremely lenient domain registrar, has been hosting [Doxbin.net](#) for years 

Communications Decency Act

- “Reiko” also shared that the reason Doxbin is not illegal, is because of Section 230 of the Communications Decency Act (CDA).
- The CDA is a US federal law which applies immunity to platforms which host or republish user’s content.
- This means that Doxbin, and other websites which republish user’s content, cannot be held legally liable for what user’s say and do.
- A case example of this, is Gamergate.

CDA 230 is a federal law that prevents websites, blogs, and forums from being held responsible for the speech of their users.

CDA 230

“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”



Death to Brianna @chatterwhiteman

7m

@spacekatgal You just made a █████ game nobody liked. That's it. Nobody will care when you die.



Death to Brianna @chatterwhiteman

7m

@spacekatgal I hope you enjoy your last moments alive on this earth. You did nothing worthwhile with your life.

Communications Decency Act

- This was a case from a female game developer Brianna Wu, against Twitter.
- She sued Twitter, as **Twitter users were sharing her dox and death threats** on the platform.
- Twitter won the case, as they **could not be held legally liable** for what user's uploaded to their platform, under the Communications Decency Act.
- Like this, Doxbin takes the stance, that even though user's upload victims doxes to their website, which can be used for harassment, they are not responsible or legally liable.

What other laws relate to Doxing?

US Interstate Communications Statute, section 875(c).

- Criminalizes any **communication containing a threat** to injure a person.
- Threatened party does not need to receive the threat.

What other laws relate to Doxing?

US Interstate Stalking Statute, section 2261A(2).

- Prohibits the use of any interactive computer service in a 'course of conduct' that places a person in **reasonable fear of death**, or **serious bodily injury**, or causes **substantial distress** to a person.

Terms of Service

Content that is not allowed on Doxbin:

Direct *threats* for physical harm

Circumventing Legal Liability

- I shared earlier that Doxbin prides themselves on being a platform where doxes are not taken down, unless it breaks their terms of service.
- Doxbin, aware of the laws discussed, has constructed their terms of service to circumvent legal liability, by **disallowing doxes to include direct threats** for physical harm.
- Whilst direct threats are not allowed, I spoke to a prolific Doxbin member called “Joana”, who shared more insights.

Do you believe Doxbin users might leverage a person's dox for intimidation or threats?



joana

Doxbin disallows **direct** threats for acts of violence.

There is no doubt that information posted on Doxbin can and has been used to harass the people it pertains to.

Circumventing Legal Liability

- “Joana” mentioned that simply sharing a victims dox could have the intention of intimidation and be used for threats.
- However, if the published dox doesn’t include a threat, it could be seen as technically complying with all US laws.
- This creates an **ambiguous stance**, as there is **nothing remaining** under US law that **prohibits Doxbin from running**.
- Whilst Doxbin will take down a dox if it violates their terms of service, they don’t proactively review any published content to see if it complies.

Rules:

Pastes that break our TOS are subject to be removed.

Here are our list of rules that you must comply with. If you don't, the paste will

Content that is not allowed on Doxbin:

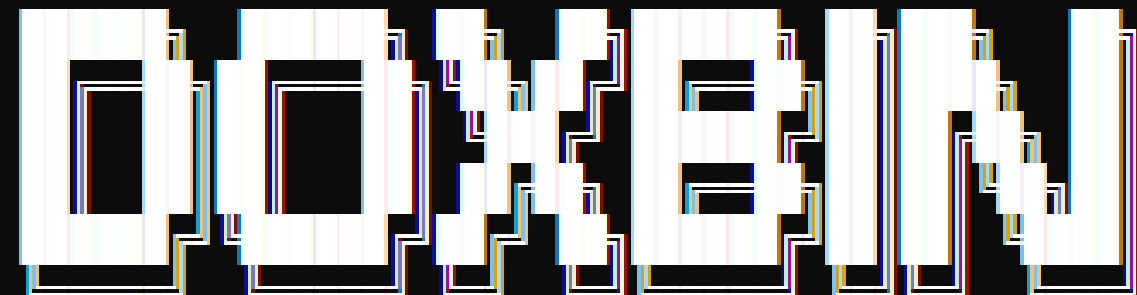
- Third party links to underage explicit images
- Pastes that don't meet our information minimum requirements (Example)
- Any personal information specifically about children under the age of 15
- Dox requests
- Spam
- IPloggers/infected files
- Reposting the same copy/paste dox
- Direct threats of physical harm, terroristic threats and swat threats/requests

If you would like to report a paste for TOS violation, contact us on Telegram

Law enforcement ONLY: [report paste report](#) (Any emails not from lawyers, police)

If a paste does not break our rules, there is nothing we can do. If you're concerned

| Title | Comments | Views | Created by | Added |
|-------------------------------------|----------|--------|----------------------------|----------------|
| Transparency Report | - | 138407 | Kt [Admin] | Jun 20th, 2020 |



<https://dox.report/> | <https://archive.is/BNgzv>

Transparency Report

We abide to a regulation made by us to comply with our current legal rights.
Please read over TOS & FAQ to understand our code of conduct.
Breaking this will result in a paste deletion.
Current Period: May 2020 - May 2024
Legal Enquiries: legal@dox.report

Updated on 18th of July, 2024

+
[September 1st, 2023]
Pennsylvania State Police, Pennsylvania, USA
Requested: Paste removal
Verdict: Denied | Information within the paste is considered public.
+

Circumventing Legal Liability

- Instead Doxbin maintains a **Transparency Report**, which is a public record of all Government agency requests to take down information on the site.
- Since inception, Doxbin has received over 141 Government requests from 27 different countries worldwide.
- However, **only 43%** of these request have resulted in a dox being taken down. This means only **60 out of a possible 165,000** have been removed.

Doxbin Responses Verdict

Pending

0.7%

Denied

19.9%



Removed

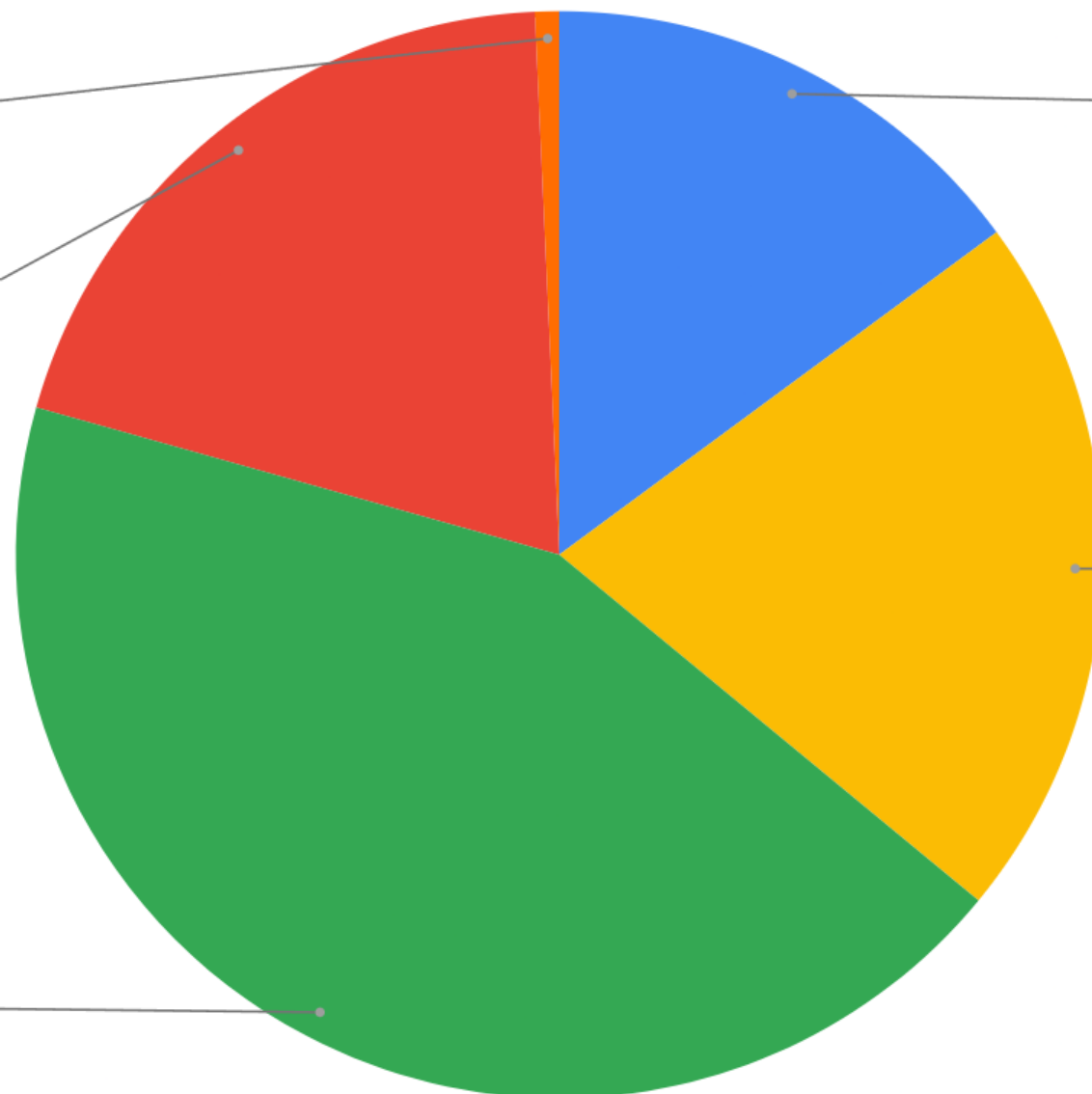
43.4%

User data not logged

14.9%

No reply

21.1%



Circumventing Legal Liability

- It's clear that Doxbin uses the Transparency Report to masquerade as running as legitimate website that complies with Government requests.
- However, they are operating in a legal gray area due to gaps in U.S. policy.
- They've carefully constructed their terms of service to exploit these gaps and avoid legal liability.
- Due to these gaps, **policy changes are required** to better protect victims, by persecuting doxing platforms and perpetrators.

Required Policy Reform

Doxing Platforms:

Hosting of doxing information, should be reasonably accepted to have the **intention of malicious dissemination** and be disallowed under communications policies.

Doxing Perpetrators:

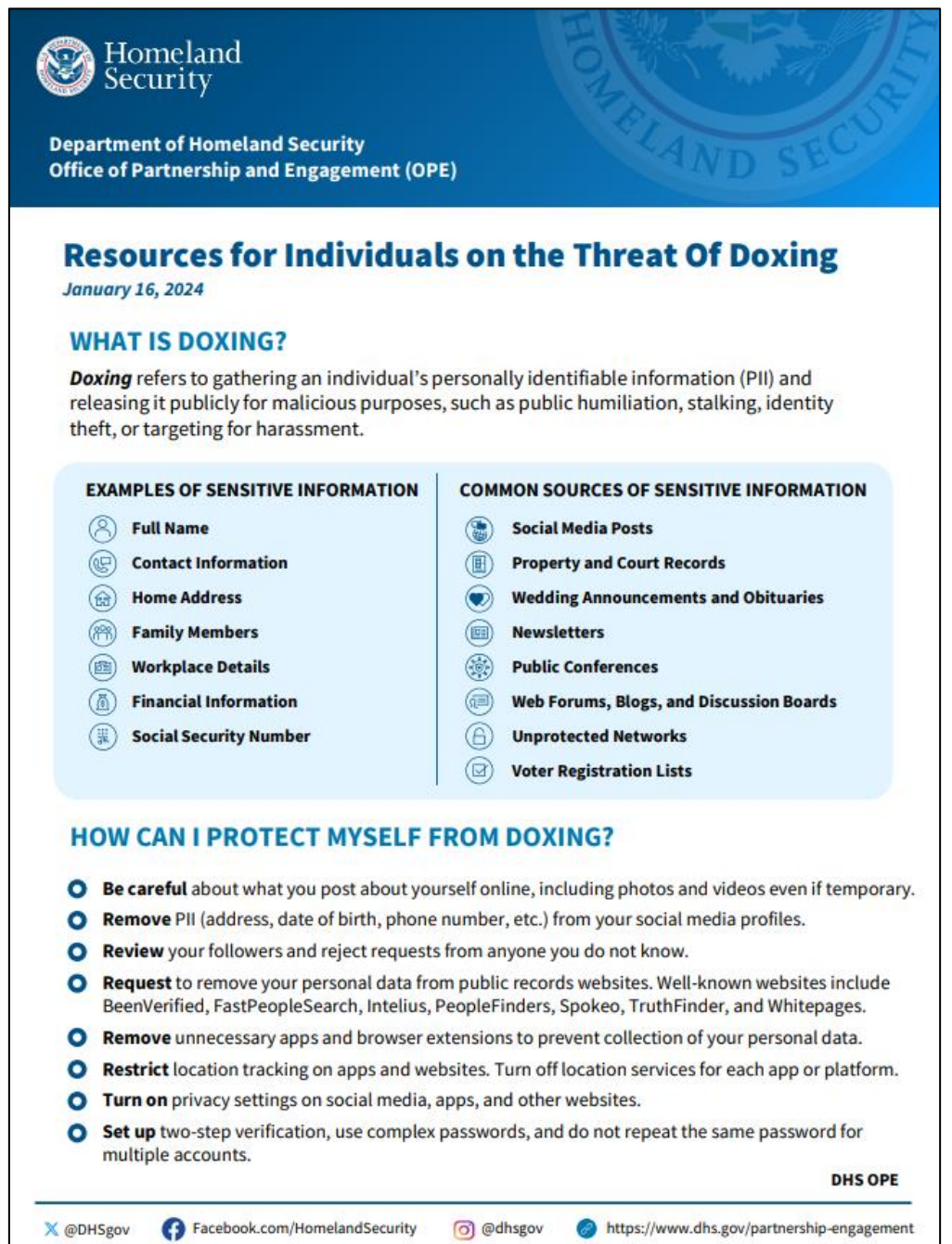
The **sharing of personal information** without an individual's permission, should be reasonably accepted to have the **intention of causing substantial stress**, or a **threat to harm** and be disallowed under stalking policies.


How to help protect yourself from Doxing?

US Department of Homeland Security

1. Turn on privacy settings on social media.
2. Set unique and complex passwords.
3. Use two-factor authentication on all accounts.
4. Limit personal information that you share online, even if temporary.

Make a habit of searching for yourself online, to see how much of your information is accessible.



 **Homeland Security**














Department of Homeland Security
Office of Partnership and Engagement (OPE)

Resources for Individuals on the Threat Of Doxing

January 16, 2024

WHAT IS DOXING?





Doxing refers to gathering an individual's personally identifiable information (PII) and releasing it publicly for malicious purposes, such as public humiliation, stalking, identity theft, or targeting for harassment.

| EXAMPLES OF SENSITIVE INFORMATION | COMMON SOURCES OF SENSITIVE INFORMATION |
|--|--|
|  Full Name |  Social Media Posts |
|  Contact Information |  Property and Court Records |
|  Home Address |  Wedding Announcements and Obituaries |
|  Family Members |  Newsletters |
|  Workplace Details |  Public Conferences |
|  Financial Information |  Web Forums, Blogs, and Discussion Boards |
|  Social Security Number |  Unprotected Networks |
| |  Voter Registration Lists |

HOW CAN I PROTECT MYSELF FROM DOXING?

- **Be careful** about what you post about yourself online, including photos and videos even if temporary.
- **Remove** PII (address, date of birth, phone number, etc.) from your social media profiles.
- **Review** your followers and reject requests from anyone you do not know.
- **Request** to remove your personal data from public records websites. Well-known websites include BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder, and Whitepages.
- **Remove** unnecessary apps and browser extensions to prevent collection of your personal data.
- **Restrict** location tracking on apps and websites. Turn off location services for each app or platform.
- **Turn on** privacy settings on social media, apps, and other websites.
- **Set up** two-step verification, use complex passwords, and do not repeat the same password for multiple accounts.

DHS OPE

 @DHSgov  Facebook.com/HomelandSecurity  @dhsgov  <https://www.dhs.gov/partnership-engagement>

What are the common mistakes you see people make that lead them to get doxed?

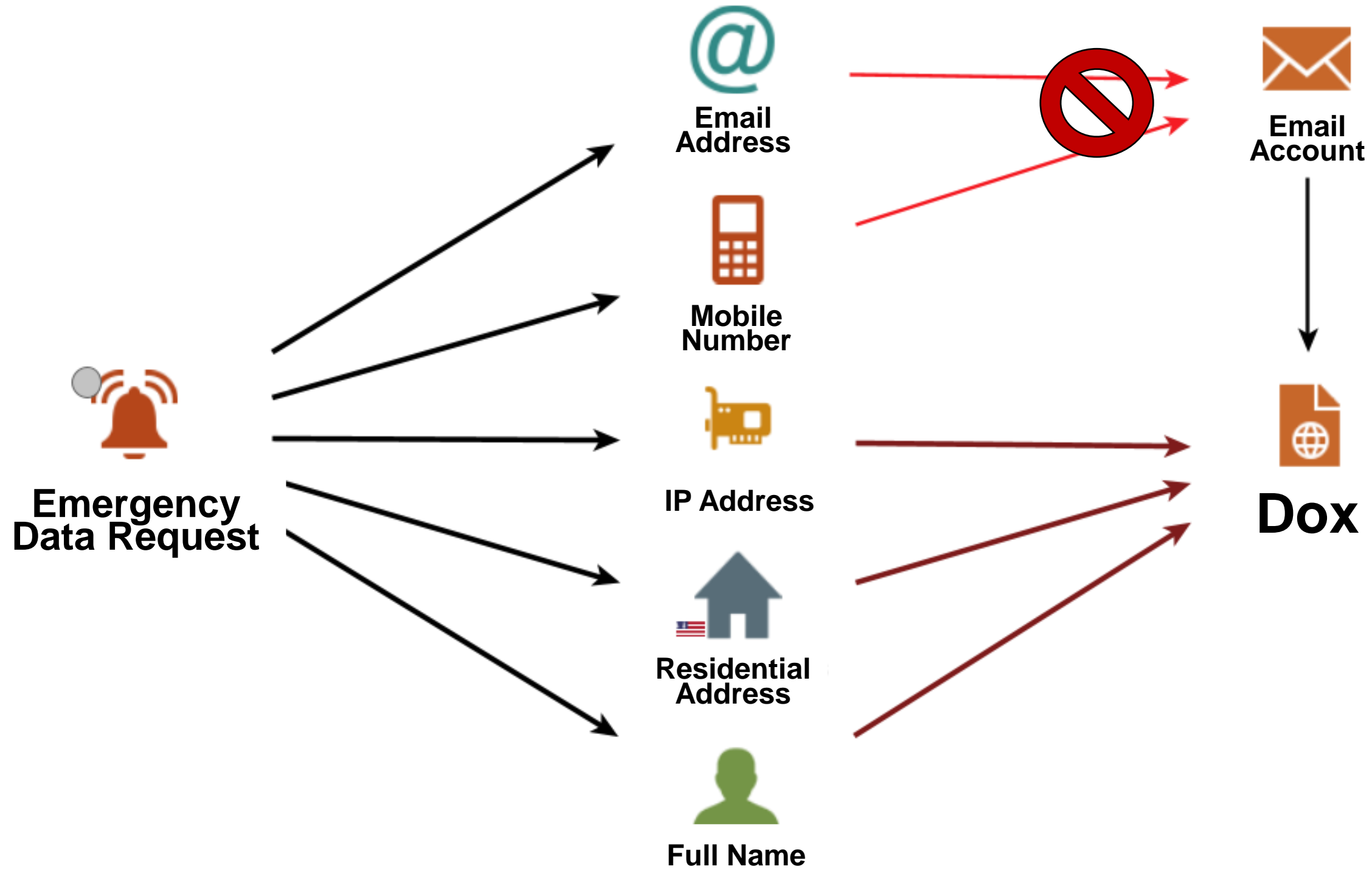


ego

- Identical email addresses across all online accounts, with password re-use.
- Using consistent or similar usernames across various platforms.
- They choose not to use VPNs.
- Sharing complete names and general location on social media platforms.
- Post personal pictures of family members, compromising privacy and security.

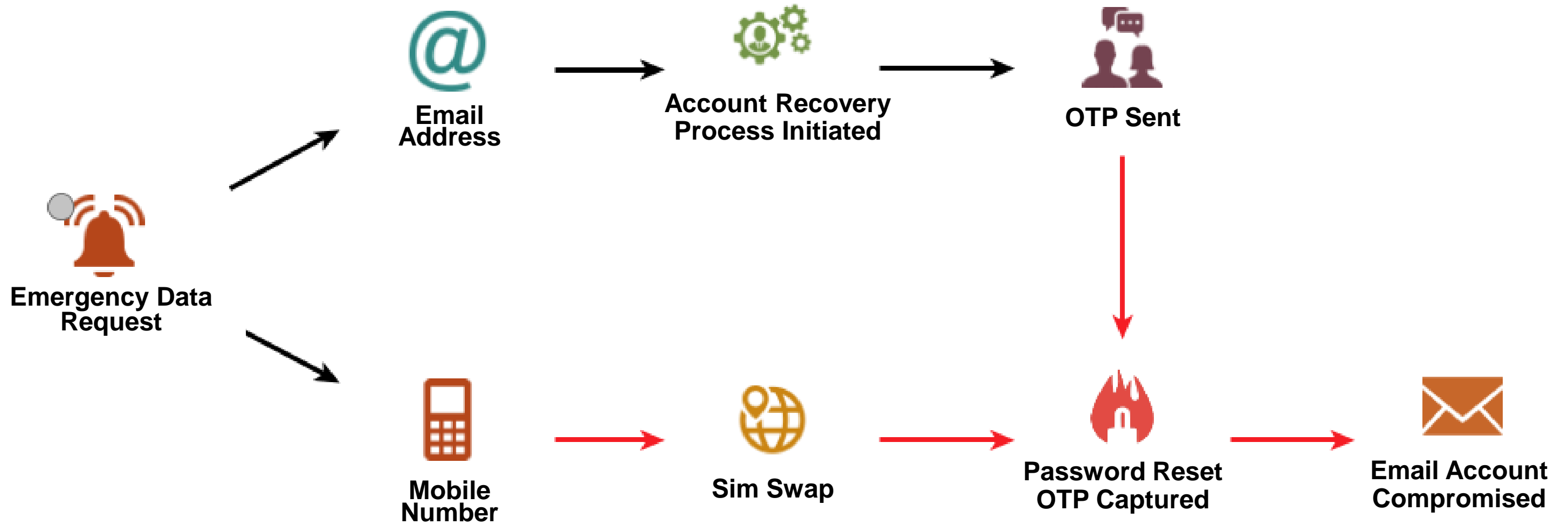
Recommendations

- Earlier I shared a diagram which shows that an adversary's primary objective after completing a fraudulent Emergency Data Request is to **compromise the victim's personal accounts**.
- Unfortunately, there isn't anything that can be done by you to protect yourself from a fraudulent Emergency Data Request, as this requires industry changes which will take time.
- Instead, you can focus on **disrupting the attack chain** which is used to compromise your personal accounts, after the fraudulent request is completed.

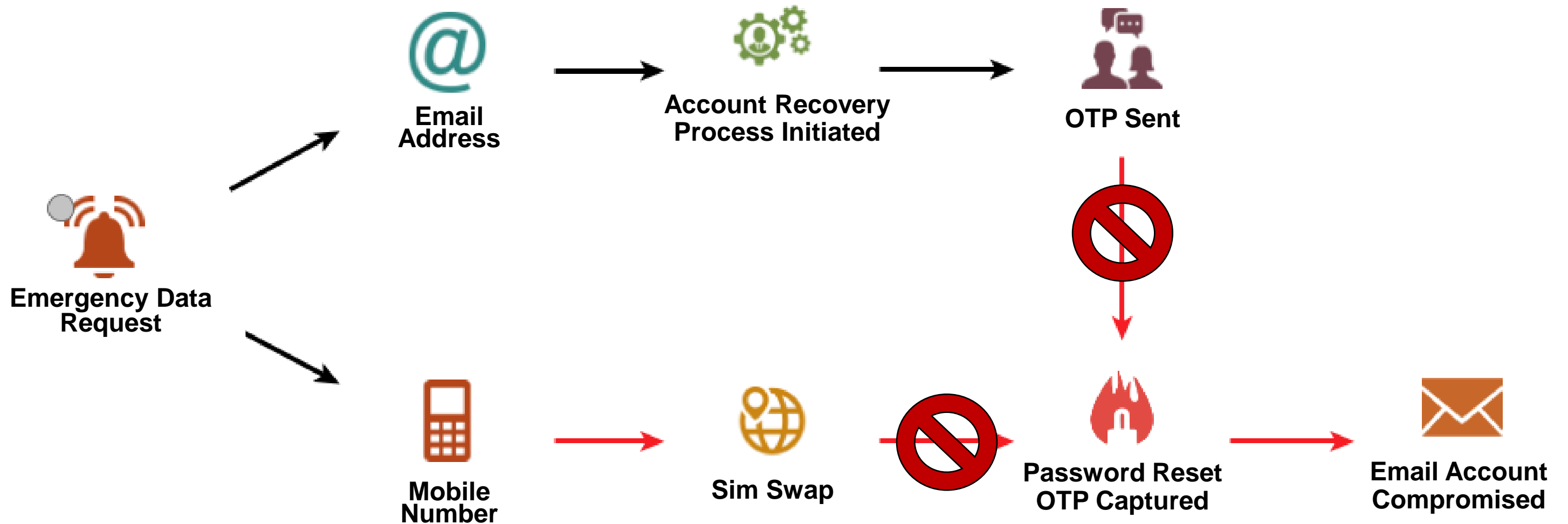


Recommendations

- When the fraudulent Emergency Data Request is completed, the adversary will obtain your email address and mobile number and use this to compromise your account through the **account recovery forgotten password** process.
- They will perform a **sim swap attack** on your mobile number, to port forward it to a sim card they control, so they can **receive a One-Time-Pass (OTP)** code.
- This OTP allows them to change the password to your account and disable multi-factor authentication, compromising it for them to harvest additional information for the dox.

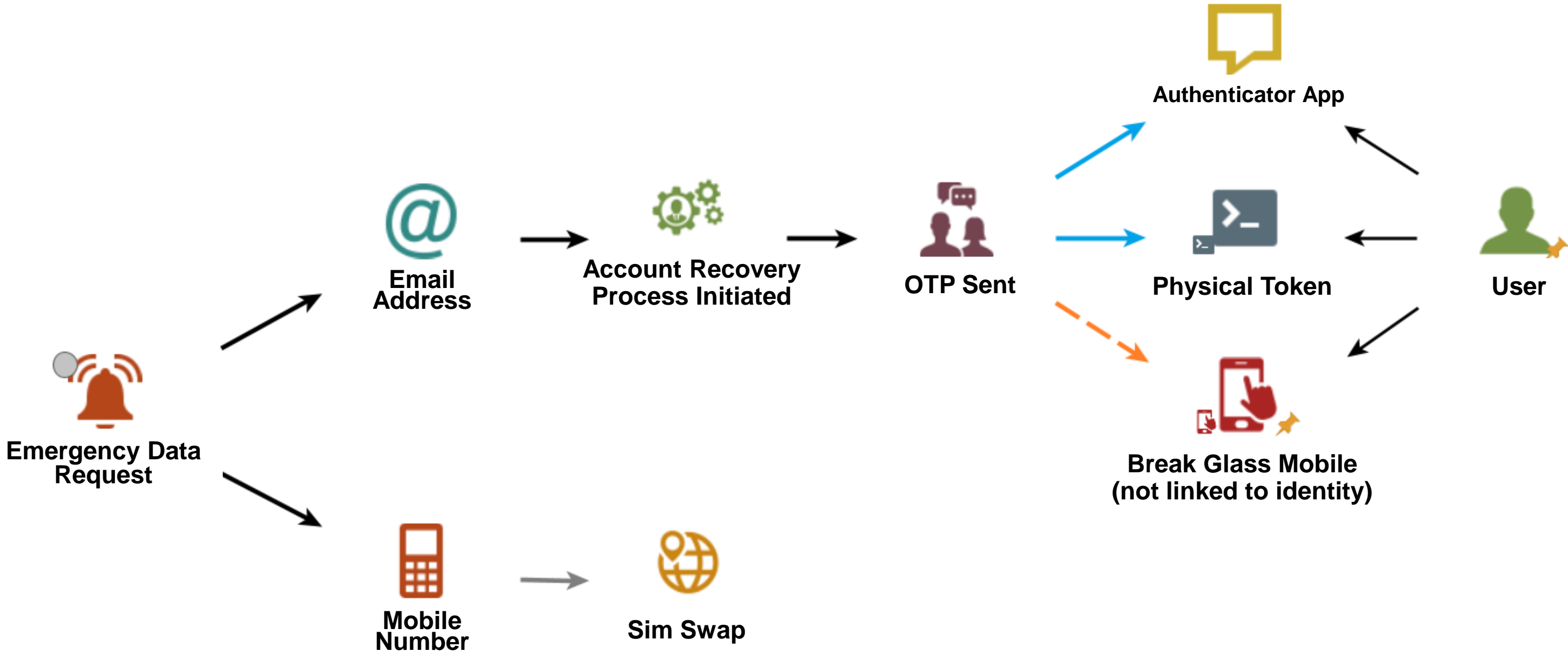


To **disrupt** the **attack chain**, you need to make sure the adversary **can't receive your OTP** code.



Recommendations

- Remove SMS-based authentication from all your online accounts.
- If a sim swap attack occurs, your mobile number can't be used to hack you.
- Your MFA must always include an Authenticator-based application, or a physical token.
- Try to never use SMS-based authentication, except in exceptional circumstances where nothing else is offered. However, the mobile number used cannot be linked to your identity in any way.



Protecting Residential Address

Google Maps

Report Inappropriate Street View

- Use P.O. boxes and mail forwarding services.
- Blur your home, vehicle and persons on google maps.



Personal Safety

Physical deterrents:

- CCTV
- Intrusion alarms
- Floodlights

Self-defence:

- Baseball bat
- Licensed firearm





- 1. Doxing is no longer just a virtual threat; it has evolved into a tool used for real world extortion.**
- 2. Limit the personal information you share and make the habit of searching for yourself online.**
- 3. Never secure your accounts with SMS-based authentication.**
- 4. Blur your home on Google Maps and implement physical deterrents.**



Read full chat
transcripts with
“Ego” and “Reiko”

larsencyber.com



Credit

1. Credit to **Zach Stanford** ([@svch0st](#)) for a massive help in the initial research phase, assisting with the preparation of interview questions, and connecting me with relevant industry professionals.
2. Credit to **Shanna Daly** ([@fancy_4n6](#)) and **Lidia Giuliano** ([@pink_tangent](#)) for their mentorship in the Black Hat Speaker's Program.
3. Credit to **Chis Rock** ([@chisrockhacker](#)) for providing feedback on my CFP submission.
4. Credit to **Angus Strom** ([@0x10F2C_](#)) for providing feedback on my CFP submission.
5. Credit to **Bex Nitret** ([@4n6Bexaminer](#)) for inspiring me to complete investigative-style security research.

References

1. Doxbin: <https://doxbin.org>
2. ViLE: <https://vile.sh>
3. Doxbin's Offshore Hosting List: <https://offshore.cat/>
4. Wired – What is Doxing: <https://www.wired.com/2014/03/doxing/>
5. DailyDot – Silk Road trial judge may have been doxed and threatened: <https://www.dailydot.com/debug/forrest-dox-threatened/>
6. Vice – What Happens When a Lawyer Takes on a Hacker: <https://www.vice.com/en/article/z4mqxy/what-happens-when-a-lawyer-takes-on-a-hacker>
7. KrebsOnSecurity – Two USA Men Charged in 2022 Hacking of DEA Portal: <https://krebsonsecurity.com/2023/03/two-us-men-charged-in-2022-hacking-of-dea-portal>
8. US Department of Justice – Two Men Charged for Breaching Federal Law Enforcement Database and Posing as Police Officers to Defraud Social Media Companies: <https://www.justice.gov/usao-edny/pr/two-men-charged-breaching-federal-law-enforcement-database-and-posing-police-officers>

References

9. US Department of Justice – Two Men Plead Guilty to Computer Intrusion and Aggravated Identity Theft for Hacking into Federal Law Enforcement Web Portal: <https://www.justice.gov/usao-edny/pr/two-men-plead-guilty-computer-intrusion-and-aggravated-identity-theft-hacking-federal>
10. NYDailyNews – Members of ViLe online group charged by Brooklyn feds with using stolen police credentials for doxing scheme: <https://www.nydailynews.com/2023/03/14/members-of-vile-online-group-charged-by-brooklyn-feds-with-using-stolen-police-credentials-for-doxing-scheme>
11. Vice – Nobody is Safe in Wild Hacking Spree: <https://www.vice.com/en/article/pkae7g/nobody-is-safe-in-wild-hacking-spree-hackers-accessed-federal-law-enforcement-database>
12. BBC – LAPSUS\$ Oxford teen accused of being multi-millionaire cybercriminal: <https://www.bbc.com/news/technology-60864283>
13. BBC – LAPSUS\$: GTA 6 Hacker Handed Indefinite Hospital Order <https://www.bbc.com/news/technology-67663128>
14. KrebsOnSecurity – NJ Man Hired Online to Firebomb, Shoot at Homes Gets 13 Years in Prison: <https://krebsonsecurity.com/2023/10/nj-man-hired-online-to-firebomb-shoot-at-homes-gets-13-years-in-prison/>
15. KrebsOnSecurity – Violence-as-a-Service, Brickings, Firebombings and Shootings for Hire: <https://krebsonsecurity.com/2022/09/violence-as-a-service-brickings-firebombings-shootings-for-hire/>

References

16. CourtListener - United States vs McGovern-Allen:
<https://www.courtlistener.com/docket/64945732/united-states-v-mcgovern-allen/>
17. YouTube: Ironic – The Dark History of Doxbin:
<https://www.youtube.com/watch?v=ULxiqLNybUA>
18. KrebsOnSecurity – Hackers Gain Power of Subpoena via Fake “Emergency Data Requests”:
<https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/>
19. US Department of Justice – Man Convicted of Violent Home Invasion Robberies to Steal Cryptocurrency:
<https://www.justice.gov/opa/pr/man-convicted-violent-home-invasion-robberies-steal-cryptocurrency>
20. WIRED – Inside a Violent Gang's Ruthless Crypto-Stealing Home Invasion Spree:
<https://www.wired.com/story/crypto-home-invasion-crime-ring/>
21. CourtListener – United States vs Seemungal:
<https://www.courtlistener.com/docket/67654880/united-states-v-seemungal/>
22. US National Institute of Justice – Ranking Needs for Fighting Digital Abuse:
<https://nij.ojp.gov/topics/articles/ranking-needs-fighting-digital-abuse-sextortion-swatting-doxing-cyberstalking>

References

23. Witwer, A. R., Langton, L., Vermeer, M. J., Banks, D., Woods, D., & Jackson, B. A. (2020). Countering technology-facilitated abuse: Criminal Justice Strategies for combating nonconsensual pornography, sextortion, doxing, and swatting. RAND.
<https://www.ojp.gov/library/publications/countering-technology-facilitated-abuse-criminal-justice-strategies-combating>
24. Australian Government eSafety Commissioner – Doxing Tech Trends and Challenges:
<https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing>
25. US Department of Homeland Security – Resources for Individuals on the Threat of Doxing:
<https://www.dhs.gov/publication/resources-individuals-threat-doxing>
26. Electronic Frontier Foundation – Section 230 Communications Decency Act:
<https://www.eff.org/issues/cda230>
27. HudsonRock – Infostealer Infections Lead to Hacking of Google, TikTok, and Meta Law Enforcement Systems:
<https://www.infostealers.com/article/infostealer-infections-lead-to-hacking-of-google-tiktok-and-meta-law-enforcement-systems/>
28. Michigan Technology Law Review – Online Harassment and Doxing on Social Media:
<https://mtlr.org/2022/04/online-harassment-and-doxing-on-social-media/>

References

29. Batuhan Kukul, Personal Data and Personal Safety: Re-examining the limits of public data in the context of doxing, International Data Privacy Law, Volume 13, Issue 3, August 2023, Pages 182-193:
<https://doi.org/10.1093/idpl/ipad011>
30. Julia M. MacAllister, The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information, Fordham Law Review, Article 44, 2017:
<https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5411&context=flr>
31. Schuster, J., Franz, A., & Benlian, A (2024). What Makes Doxing Good or Bad? Exploring Bystanders' Appraisal and Responses to the Malicious Disclosure of Personal Information
<https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/5d7c2c85-a253-4b5c-9728-a6c2a614a5d0/content>
32. Shan, G., Pu, W., Thatcher, J. B., & Roth, P. (2024). How Doxing on Social Media Leads to Social Stigma and Perceived Dignity.
<https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/3607365d-95e3-4b0a-ae96-84045e78e07e/content>