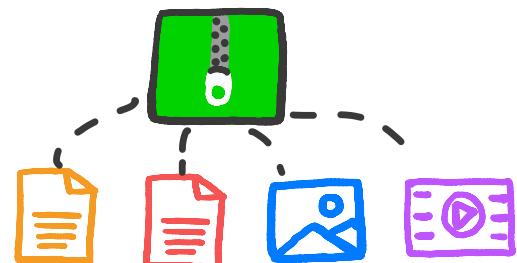


Phishing Campaign

Hunting Phishing Sites in the Wild without Phishing Kit

Ready-made
templates & scripts

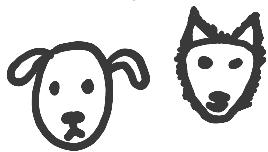


by
@thebitdoodler



Beyond the Bio

Pet Parent



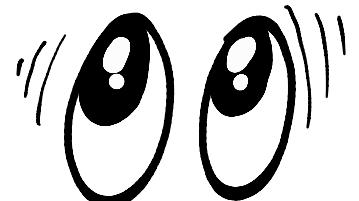
Doodler



Security Researcher

Biker

Co-founder @SecurityZines.com

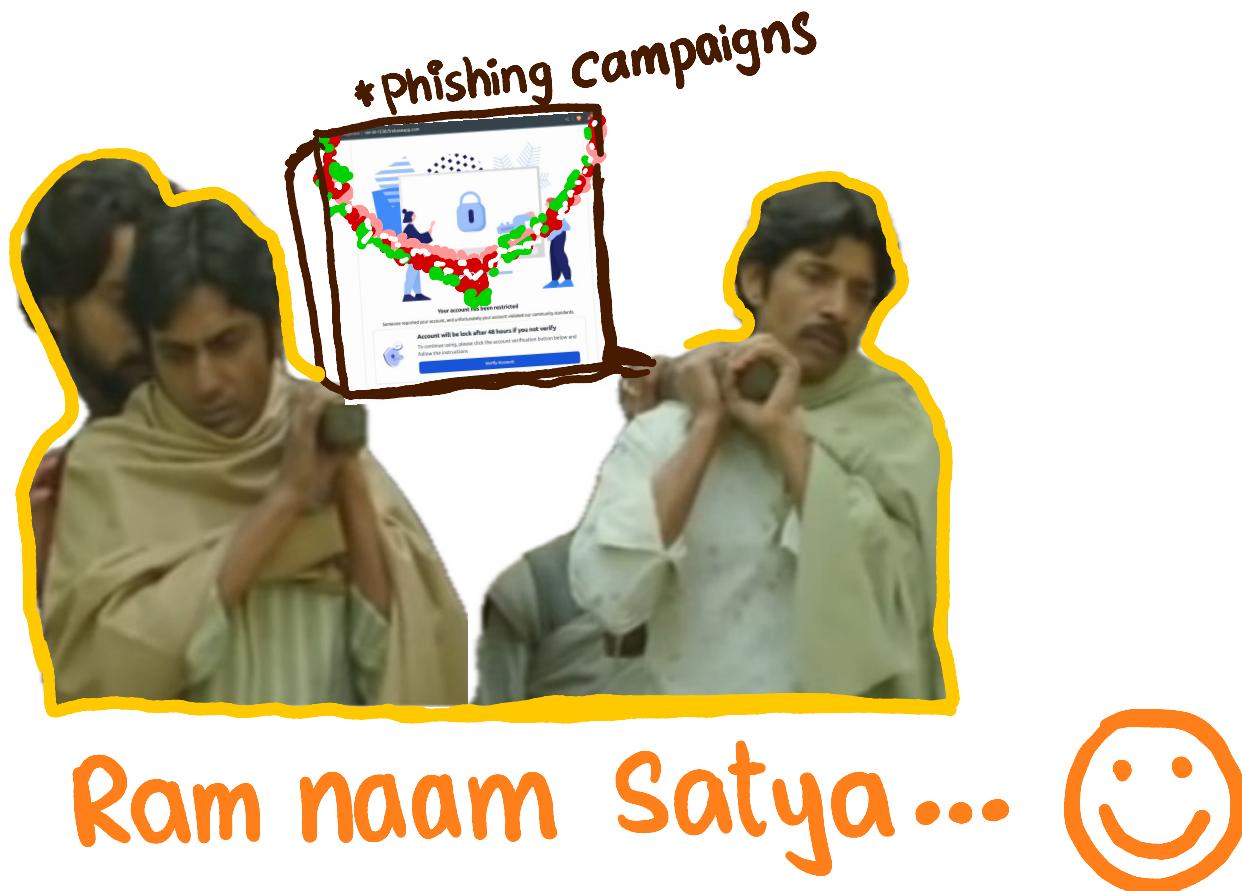


Agenda

- Basic Structure of a Phishing Site
- Phases of a phishing Campaign - from an Actor's Lens
- How to get an active phishing Link
- Analyzing the phishing site
- Automation



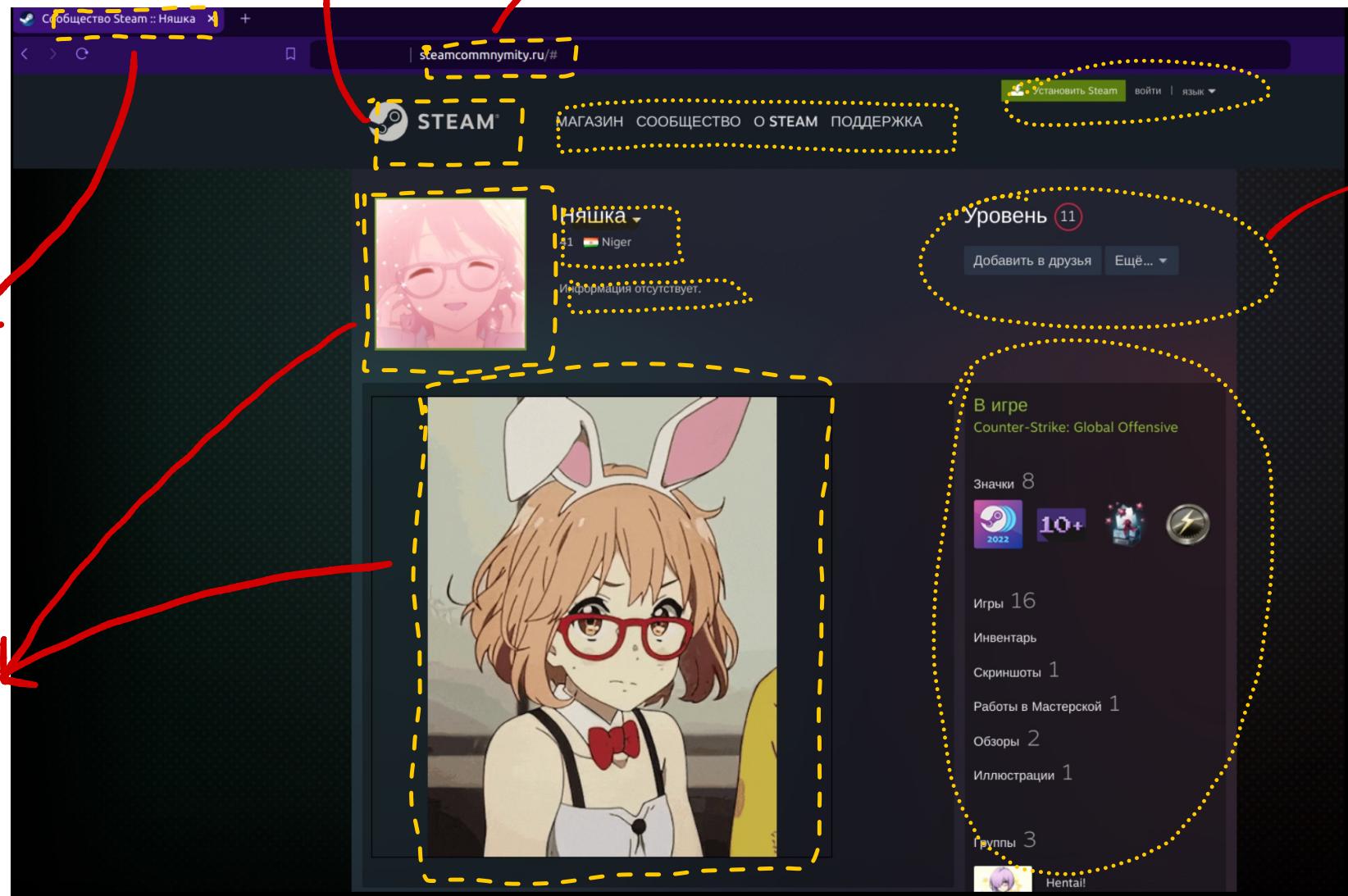
main Agenda



"oo'"

Basic Structure of a Phishing Site





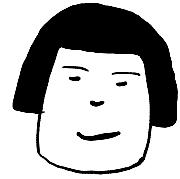
Site
Title

Logo

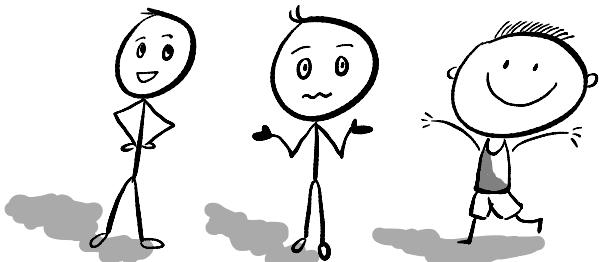
URL

Rendered
Text

Images

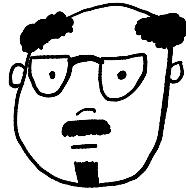


Phases of a Phishing Campaign



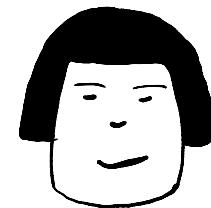
① Selection of a target

- Trends
- user base
- Financial gain



② Create / find a phishing kit

- Buy /clone
- Obfuscation
- necessary Config



③ Selection of Infrastructure

- Less regulation
- Shady / self-owned infra
- Freemium Services

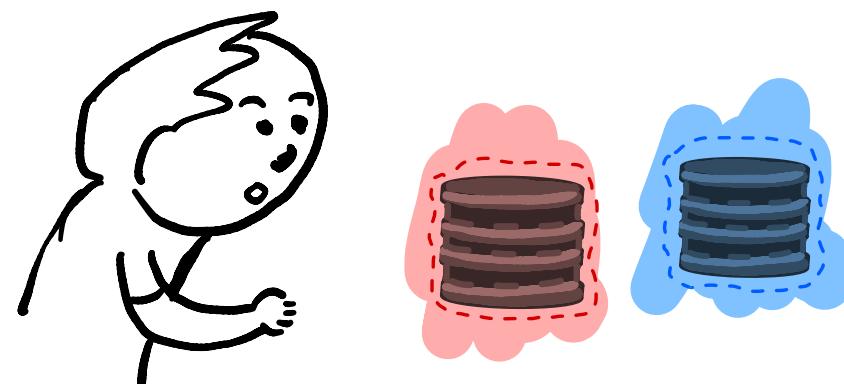


jor jor se bolke sabko scheme bata de

④ Find distribution medium

- SMS
- Email
- Social media
- SEO Poisoning

How to Get an Active Phishing Link



Open Source ❤

GitHub

Search "Phishing database"

Search "Phishing Feed"

GitHub search results for "Phishing database". The search bar at the top has a yellow dashed box around it. The results show 80 repositories. One repository, "mitchellkrogza/Phishing.Database", is highlighted with a yellow dashed box. It is described as a "Phishing Domains, urls websites and threats database". Another repository, "d3sign/disallowed-usernames", is also highlighted with a yellow dashed box. It is described as an "open source database of disallowed usernames for software projects to prevent phishing and impersonation". The sidebar on the left shows filters for Code, Repositories, Issues, Pull requests, Discussions, Users, and More. The Languages section includes Python, JavaScript, HTML, Jupyter Notebook, PHP, Shell, Go, Java, TypeScript, C#, and More languages... Advanced filters include Owner, Size, Number of followers, and Number of forks.

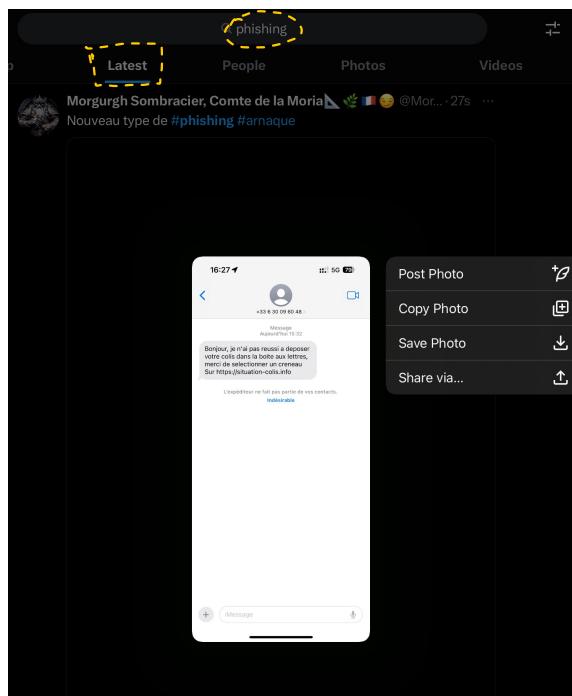
GitHub search results for "Phishing feed". The search bar at the top has a yellow dashed box around it. The results show 18 repositories. One repository, "409H/PhishingFeed", is highlighted with a yellow dashed box. It is described as a "simple project intended to automatically combine multiple phishing intelligence feeds into a single set of ...". Another repository, "kurobeats/phishing_hosts", is also highlighted with a yellow dashed box. It is described as a "host file generated from updated phishing site feeds". The sidebar on the left shows filters for Code, Repositories, Issues, Pull requests, Discussions, Users, and More. The Languages section includes Python, Jupyter Notebook, Shell, and More languages... Advanced filters include Owner, Size, Number of followers, Number of forks, Number of stars, Date created, Date pushed, Topic, License, Archived, and Public.

Open Source ❤

Twitter/x

Search

x.com/explore > "phishing" > latest



Accounts

@PhishFort

@noladefense

@PhishStats

@PhishFindR

@illegalFawn

Open Source ❤

PhishTank

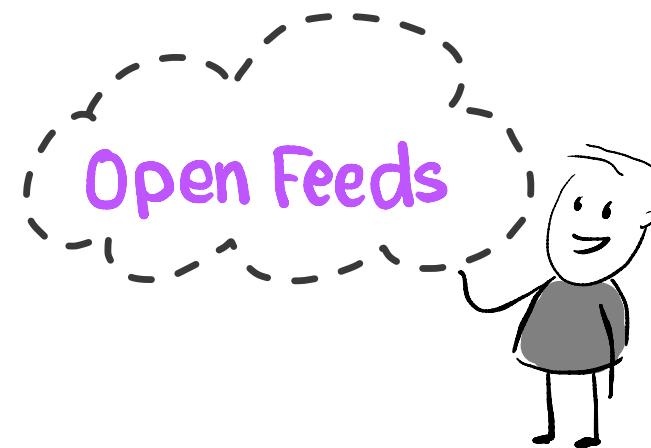
- Community Based by Cisco Talos Intelligence Gp.
- Provides API access

OpenPhish

- Free to use
- Community Feeds

AlienVault OTX

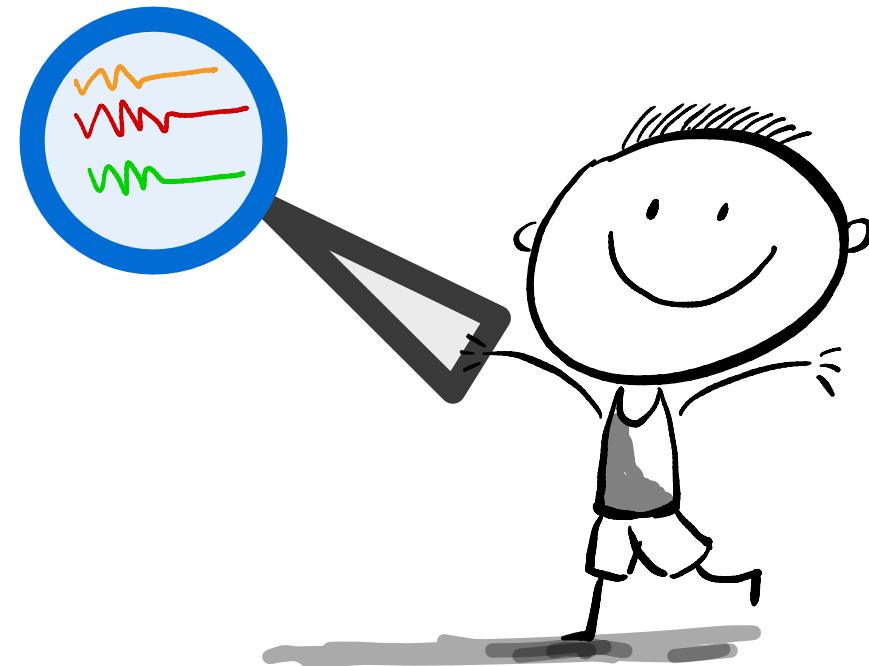
- Community driven
- owned by AT&T
- Malicious & Phishing



Urlhaus

- Malicious feeds
- Abuse.ch

Analyzing a Phishing Site



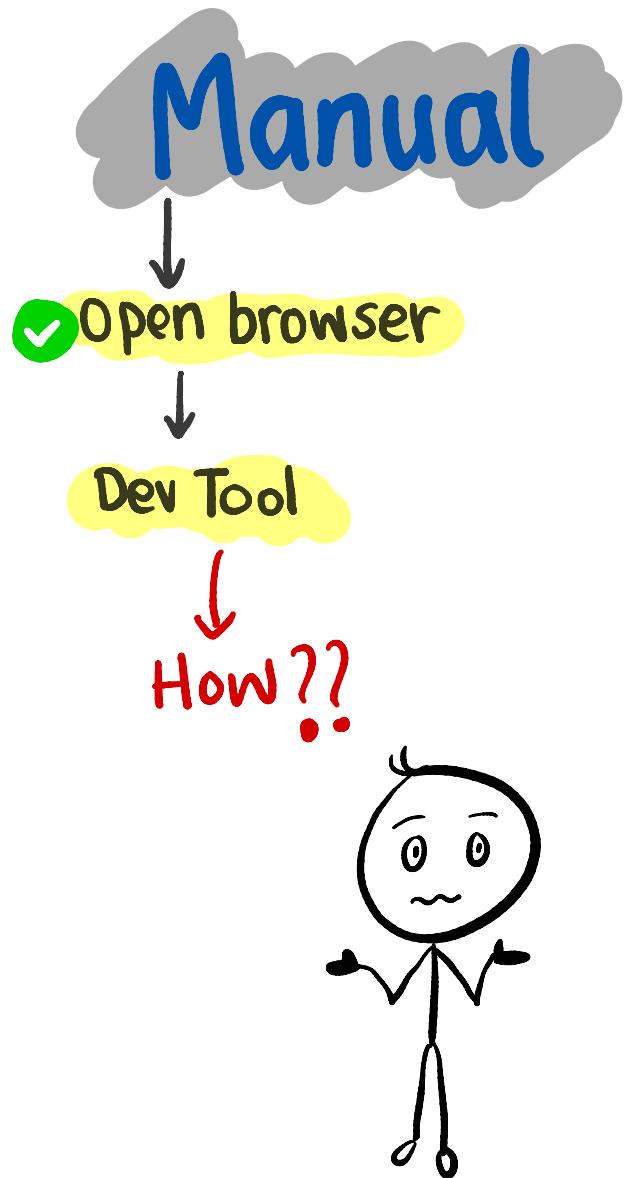
Manual

Open browser

the phishing URL

Dev Tool

Automated



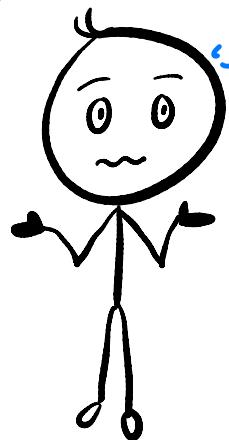
Automated

Manual

✓ Open browser

Dev Tool

How??



Automated

+ shift + i



Manual

Open browser

Dev Tool

Look for...

Automated

Manual

Open browser

Dev Tool

Look for...

URL → Certificate
domain Whois

Automated

Manual

Open browser

Dev Tool

Look for...

URL → Certificate
domain Whois

Assets
image JS other files

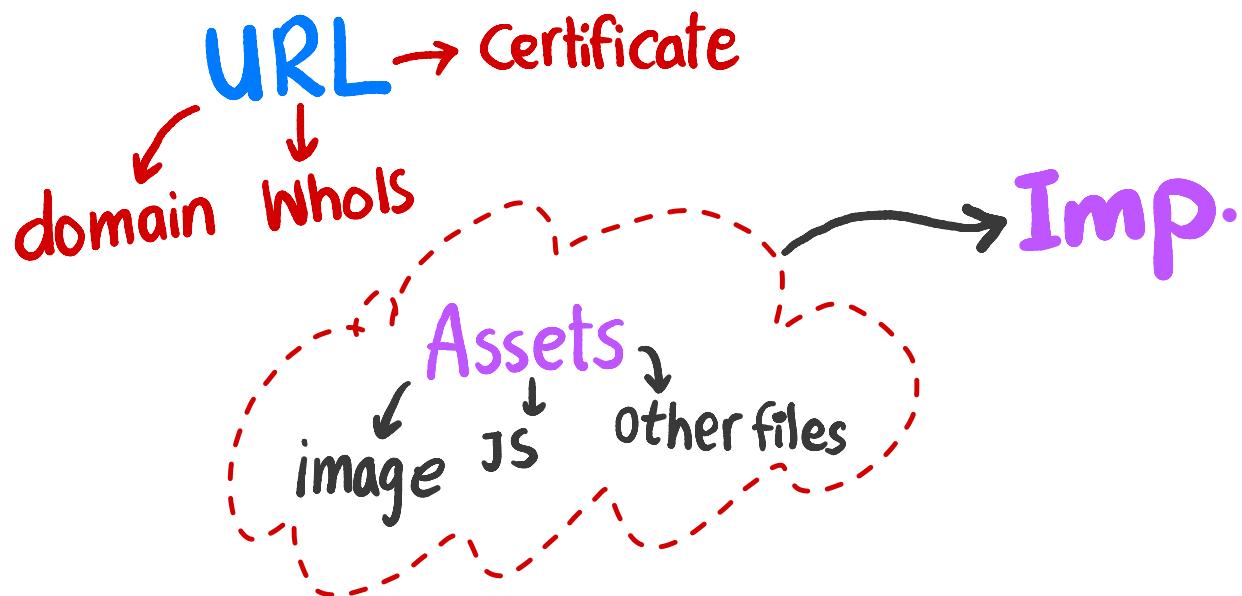
Automated

Manual

✓ Open browser

✓ Dev Tool

Look for...



Automated

Manual

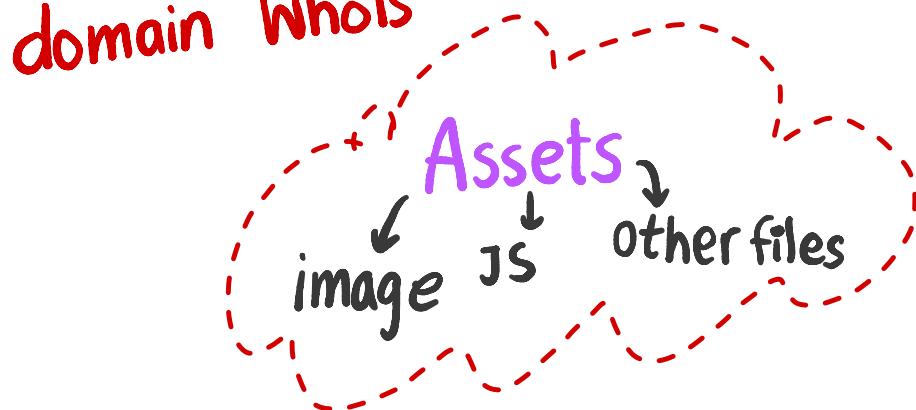
✓ Open browser

✓ Dev Tool

Look for...

URL → Certificate

domain Whois



Automated



Karte Kuch
prabandh...

Mere pas ek
mast plan h ...



DEMO
aapke screen pe ye raha...

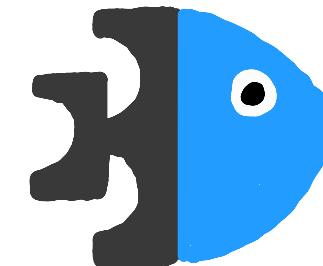
"aayien"



Automation



urlscan.io



ChekPhish.ai



phish.report



Demo Time

Ab underground hone Ka
samay aa gya h...

(





Thik Hai Bhai!
Mai Chalta Hoon...

you can't see my tweets



if don't follow **ME**

@thebitdoodler



DM's are open