HIDDEN IN PLAIN SIGHT

HOW ADVERSARIES HIDE THEIR MALICIOUS CONTENT ONLINE

BY NATE BALMAIN

Center for Security and Privacy

Story

- On June 1, 2023 the Oregon DMV learned that they were a part of a global hack of the MOVEit file transfer program
- On June 12th ODOT confirmed information was accessed
- **CVE-2023-35708** was SQL-Injection Vulnerability
- The Adversaries have this information what are their options?
  - Sell it
  - Steal Peoples Identities
- This presentation focuses on the former

Definition of terms

- Adversary:

  One who is engaged in hosting, searching for, or attempting to communicate with other adversaries for the purposes of obtaining malicious content.

- Malicious Content:

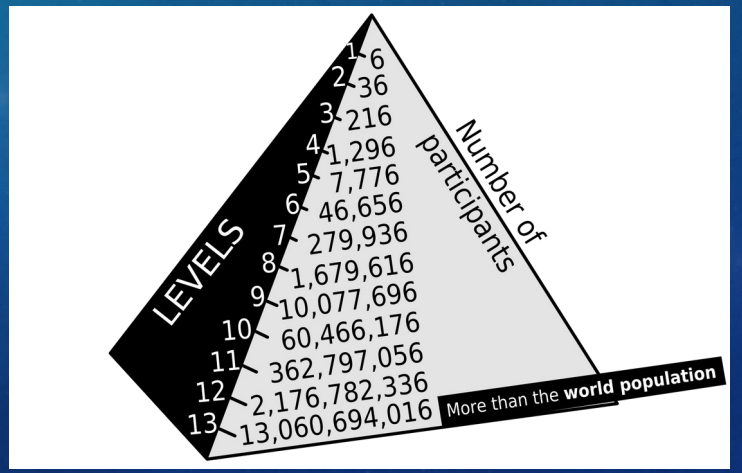
  Computer Malware, other’s personal information, illicit imagery, content related to harming others, or is otherwise illegal to communicate, obtain, or have.

- Malicious Website:

  Websites containing malicious content

Advertising of Malicious Content

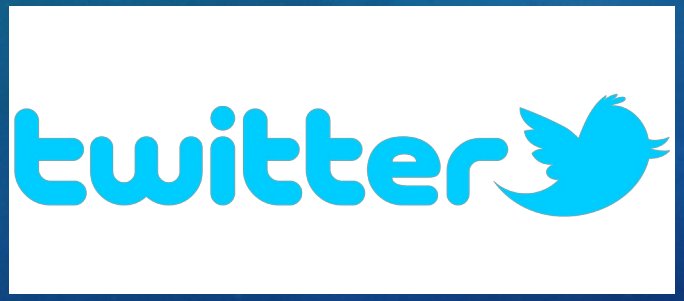
- While adversaries are not likely to use ‘main stream’ advertising, they still may advertise on friendly malicious websites or social media.
- Advertising can be as simple as “Have content for sale, here’s my info”
- Or “visit [site] for content”
- Get users to mass spam invited links for access to more content.
  - See Internet Watch Foundation (IWF) iCAP



Social Networks

Social Networks

- Facebook and Twitter are large social networks with large content moderation teams.
  - Only a matter of time before they find the bad content.
  - Possible large visibility and reach, easy to get caught.
- Truth Social… exists….
- Mastodon instances are a better choice.



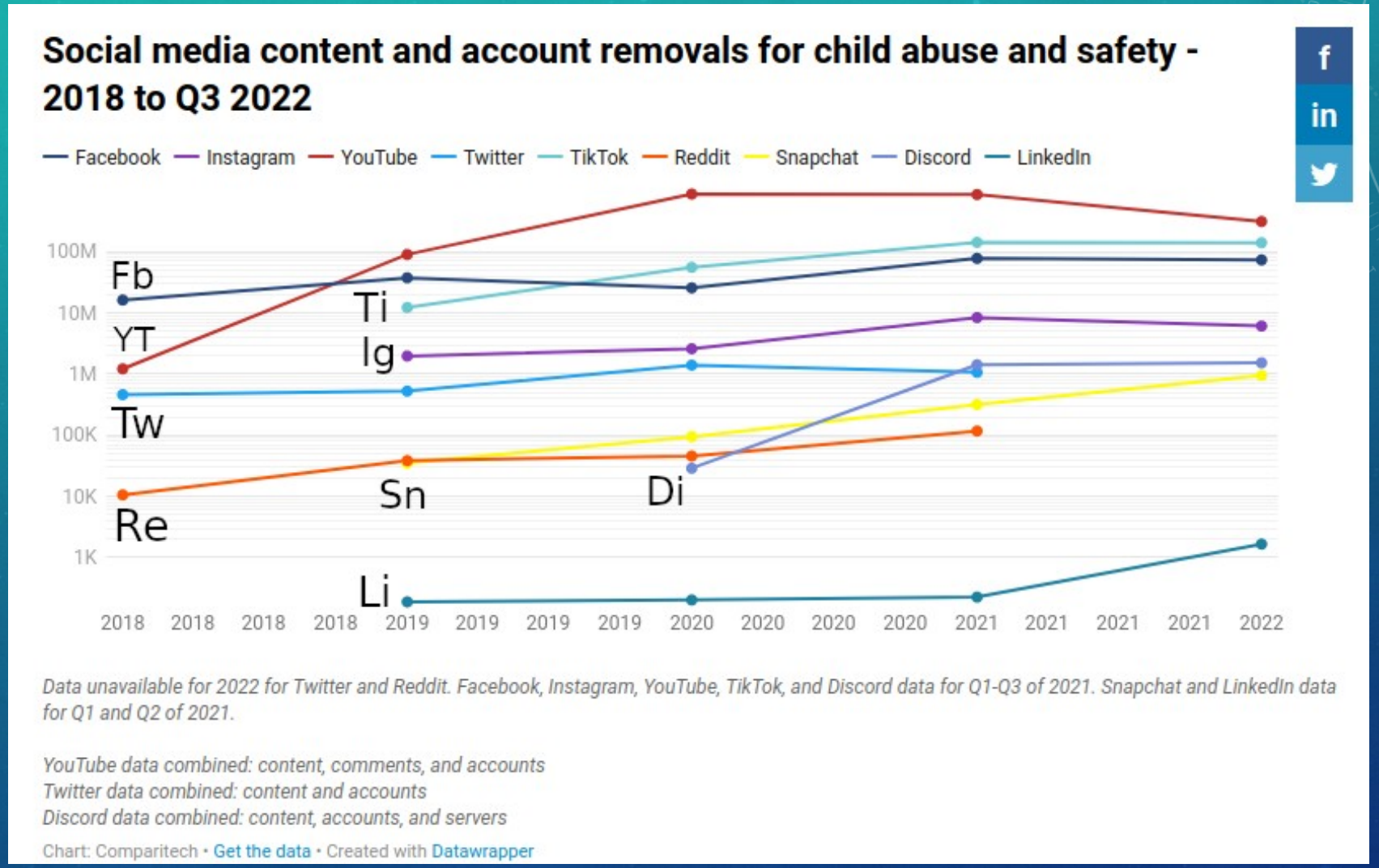


Chart from comparitech

What can we do with large social media

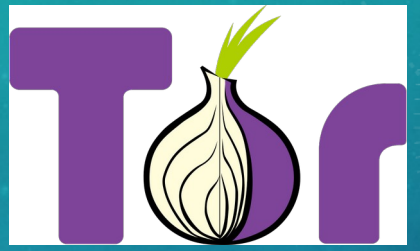
- Report content as we see it using builtin reporting features
- Cyber tip
- There are many papers on detecting fake accounts
  - Kupershtein, Leonid & Voitovych, Olesya & Vitalii, Holovenko. (2022). DETECTION OF FAKE ACCOUNTS IN SOCIAL MEDIA.
  - Shamseddine, Jad & Malli, Mohammad & Hazimeh, Hussein. (2022). Survey on Fake Accounts Detection Algorithms on Online Social Networks
- Develop better tools to automatically detect malicious content
- IP Ban users in repeated violation

Encrypted Telecommunications and Web Traffic

Encrypted Telecommunications

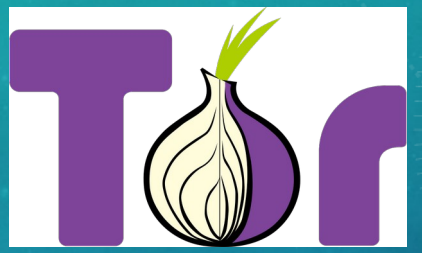
- Encrypted telecommunications enable people to communicate with one another in a more private manner
- Messages are encrypted to ensure that they cannot be sniffed out, Adversary in The Middle (AiTM) style
- Examples include
  - Signal, Telegram, WhatsApp, many more.
- Some apps offer End To End Encryption (E2EE) meaning the message is encrypted before it leaves the device
- Others use Client/Server encryption
- Self-deleting messages

Encrypted Web Traffic (Tor)



- Well-known already
- Onion sites are only accessible through the Tor network
- Used for good reasons and bad
  - Free speech, escape state censorship, find non state-sponsored information.
    - Journalism
  - Purchase illegal goods, host illicit content, “rent-a-hacker,” etc.
- Only ~6.7% of Tor users globally use it for malicious purposes.
  - Study in Proceedings of the National Academy of Sciences
- Low bar to access and use, hard to find.
- Most results on the Tor Anonymity Network are not accessible to the “clear web”

Encrypted Web Traffic (Tor)



- Tor is still used for malicious content
- Internet Watch Foundation (IWF) identified 1067 new hidden services in 2022 used for malicious content
- Used to host botnets
- Network / Content Patterning or infiltration can be used to unmask these hidden services

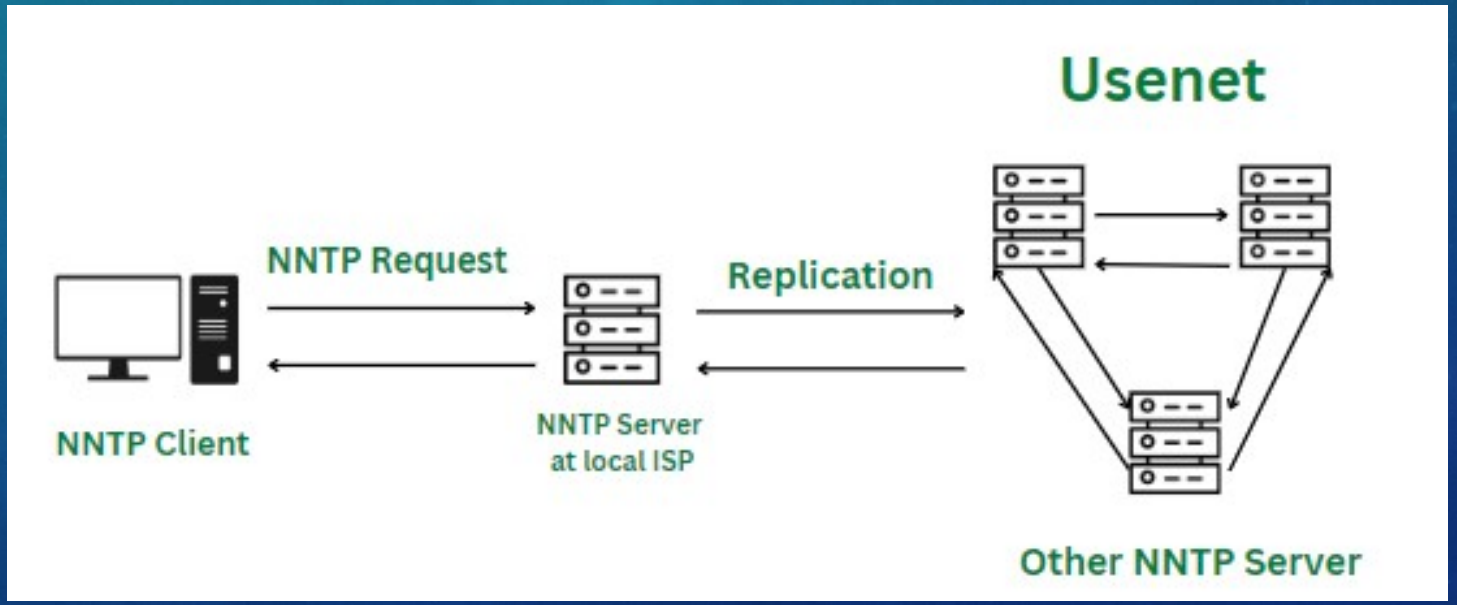
Torrents and Usenets

Torrents and Usenets

- Usenets are similar to Torrents but there are some differences.
- “There are two controversial issues attached to writing about Usenet:

  1) the first rule of Usenet is that you don't talk about Usenet, and

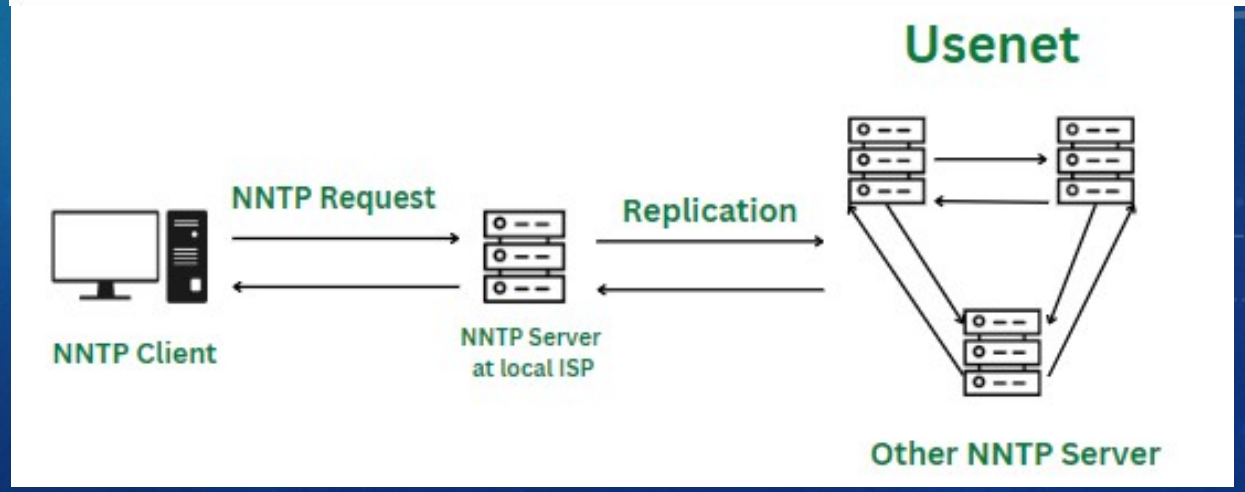
  2) it's commonly used to download copyrighted material” [lifehacker.com].



What is a Usenet?

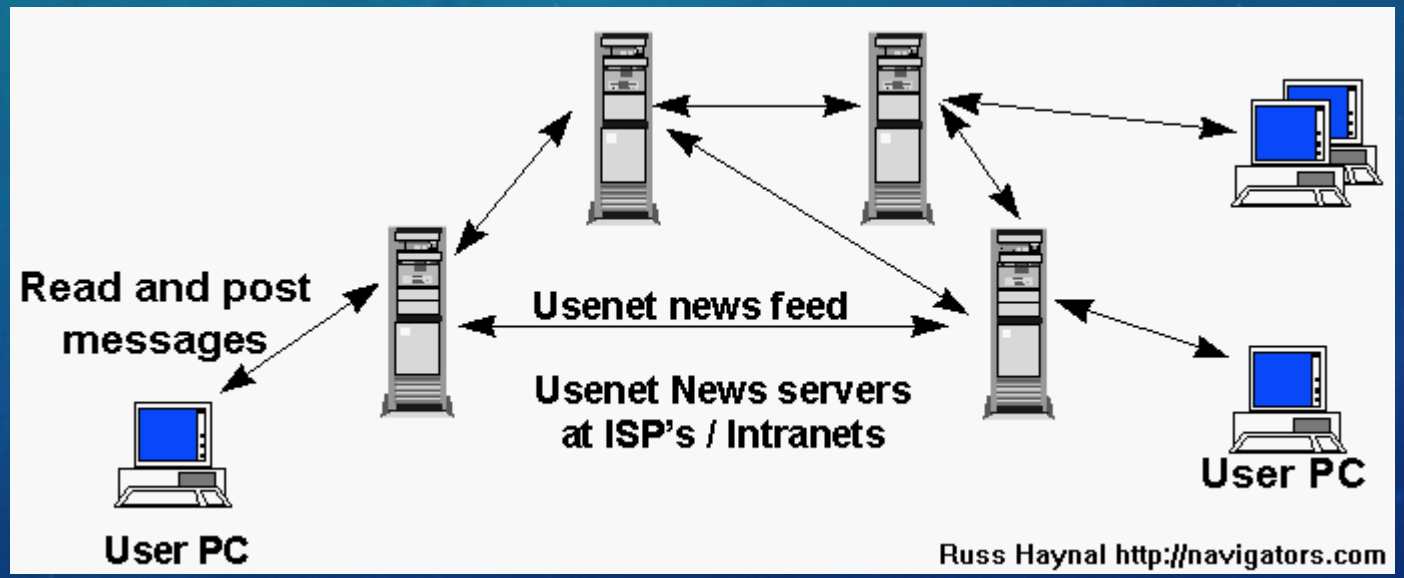
- Precursor to web forums
- Allow users to read and post on topic categories
- Resembles a bulletin board system
- Threaded discussions
- Newsgroups
- NNTP
  - Network news transfer protocol

```
OA [  58: Plain Text              ] Geminisphere via backlinks
O      [   9: Andy Burns             ]
O          [  26: news@zzo38computer.org.]
O          [  24: Leo                    ]
=>     [  35: => comp.infosystems.gem] []
O  [  92: <joe@example.invalid>  ] teletext-ish pages?
 U:---  c.i.gemini [14]    Top (5,39)     (Summary Plugged Undo-Tree) Wed Mar
From: rtr <rtr@balaraw.invalid>
Subject: Re: Geminisphere via backlinks
Newsgroups: comp.infosystems.gemini
Date: Sun, 27 Feb 2022 20:34:06 +0800 (4 weeks, 2 days, 14 hours ago)
Organization: Aioe.org NNTP Server

Plain Text <text@sdfeu.org> writes:

> Got a proof-of-concept working of a pingback script that accepts
> URLs (backlinks) of reply posts and checks the remote content for
> a => link to one's capsule before appending the URL to the list of
> received replies.
>
> Maybe others want to expand on that for their own pleasure.
> Cheers
>
> On 2020-11-13, in the mailing list:
>> If clients would send referers, servers could collect (cache) and
>> present those to clients asking for links to the current page
 *:---  c.i.gemini Re: Geminisphere via backlinks   Top (6,0)      (Article U
```



How much copyrighted content is on Usenet?

- In a lawsuit Perfect 10 (an adult entertainment magazine) claimed that Giganews (a Usenet provider) “offers 25,000 terabytes of copyrighted materials.” Perfect 10, Inc. v. Giganews, Inc. (9th Cir. 2017) p. 26
- Perfect 10 lost the case.
- IWF found 17 newsgroups on Usenet with malicious content in 2022.



Usenet

- Law enforcement can work with Usenet providers to find and shut down newsgroups with malicious content on them and users who post it.
- Members of newsgroups can report content to the appropriate location
  - Usenet Provider / Indexer
  - DMCA
  - Cyber Tip
    - National Center Missing Exploited Children (NCMEC)
    - Internet Watch Foundation (IWF)

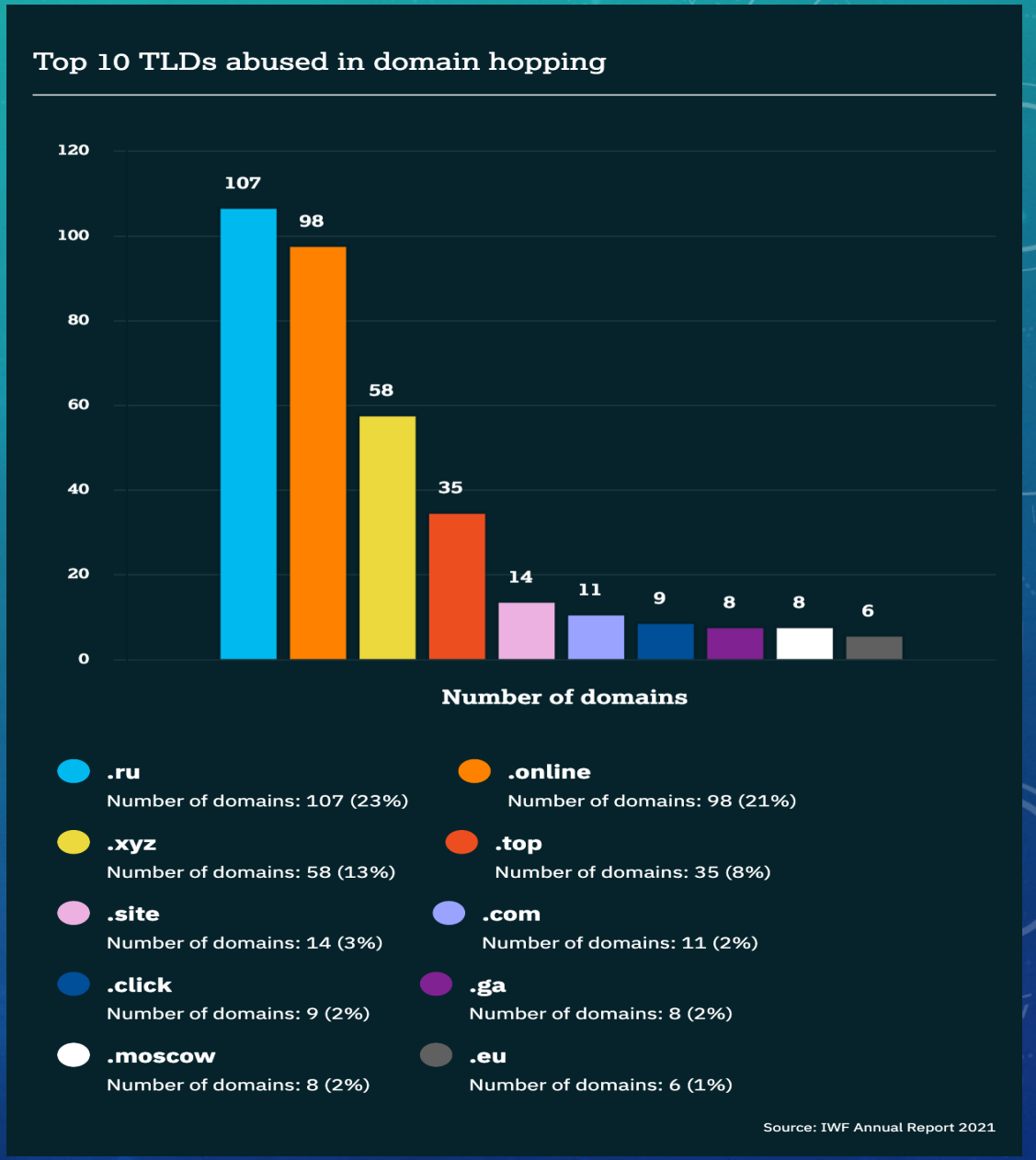
CLEAR WEB

Top Level Domain Hopping

- “...when a site (e.g. ‘badsite.ru’) keeps its second-level domain name (‘badsite’) but changes its top-level domain (‘.ru’), creating a whole new website with different hosting details but retaining its ‘name brand’. So from ‘badsite.ru’, the additional sites ‘badsite.ga’, ‘badsite.ml’ or ‘badsite.tk’ could be created. This allows instances of a website to persist online after the original has been taken down while keeping the website recognizable and easy to find.” (IWF, 2021)
- Similar to the legitimate practice of Registrar Hopping

Top Level Domain Hopping What can we do?

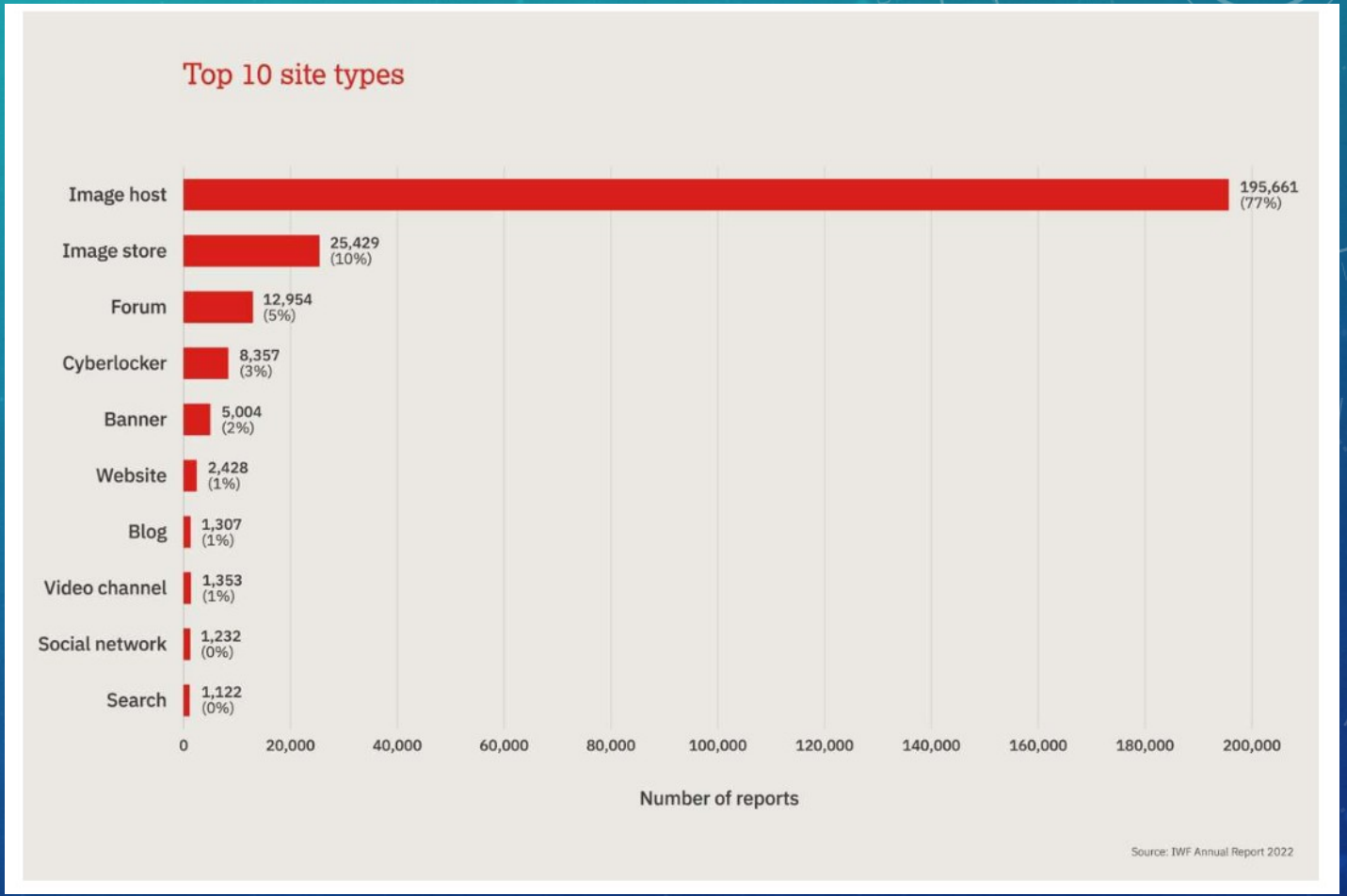
- When registrars or law enforcement take down a website, take down the second level name (badsite from previous slide) instead of just the TLD.
  - Impersonated sites could get caught in this ‘scorched earth’ approach.
  - A more sophisticated approach is needed to combat this.
- Targeted Monitoring of abused TLDs; where reasonable
- A second level name ‘blocklist’



Have someone else host the content for you

Source IWF

- The security company Sucuri detected 10,890 infected websites from September 2022 - February 2023
  - AdSense fraud campaign
- IWF received 392 reports between June – December 2013 relating to personal or small business websites being hacked for purposes of distributing malicious content.
  - Content stored in orphan folders
  - Downloading content also downloaded a Remote Access Trojan (RAT)



Role of Hosting Providers

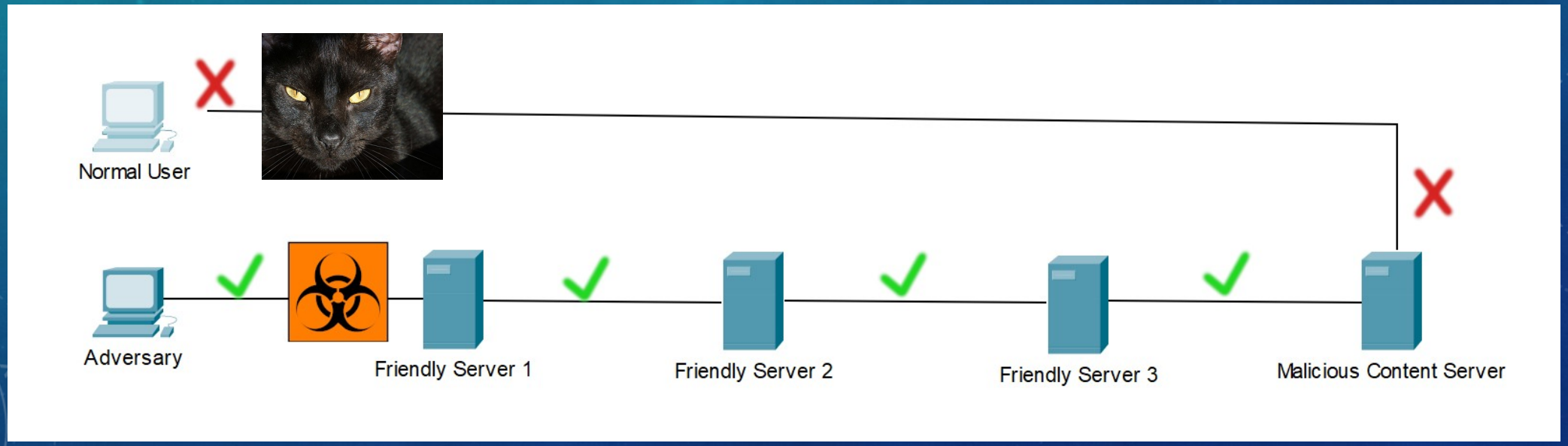
- A study published in 2013 studied hosting providers responses many security events
- Many hosting providers used verification as a means to ward malicious use (preventative measure)
- Only one provider tested notified clients when website was compromised
- One regional provider took action without notifying the client; deleting all files (including clean ones)
- 21/22 tested providers either did not run an antivirus scan monthly or were using invalid signature sets for said scan
- None of the providers considered multiple outgoing connection attempts to an IRC server suspicious

Why is it this way?

- A security researcher at Malwarebytes looked into this as well.
- Two camps of website hosting providers
  - Those who did not care where the money came from; did not cooperate
  - Those who actively respond to abuse notifications and do cooperate.
- Recommendation: people who are hosting or looking to host their website should look into the hosting provider's response to abuse / takedown notices.
  - Companies with bad reputation should be avoided
- Legislation
  - Slow but necessary

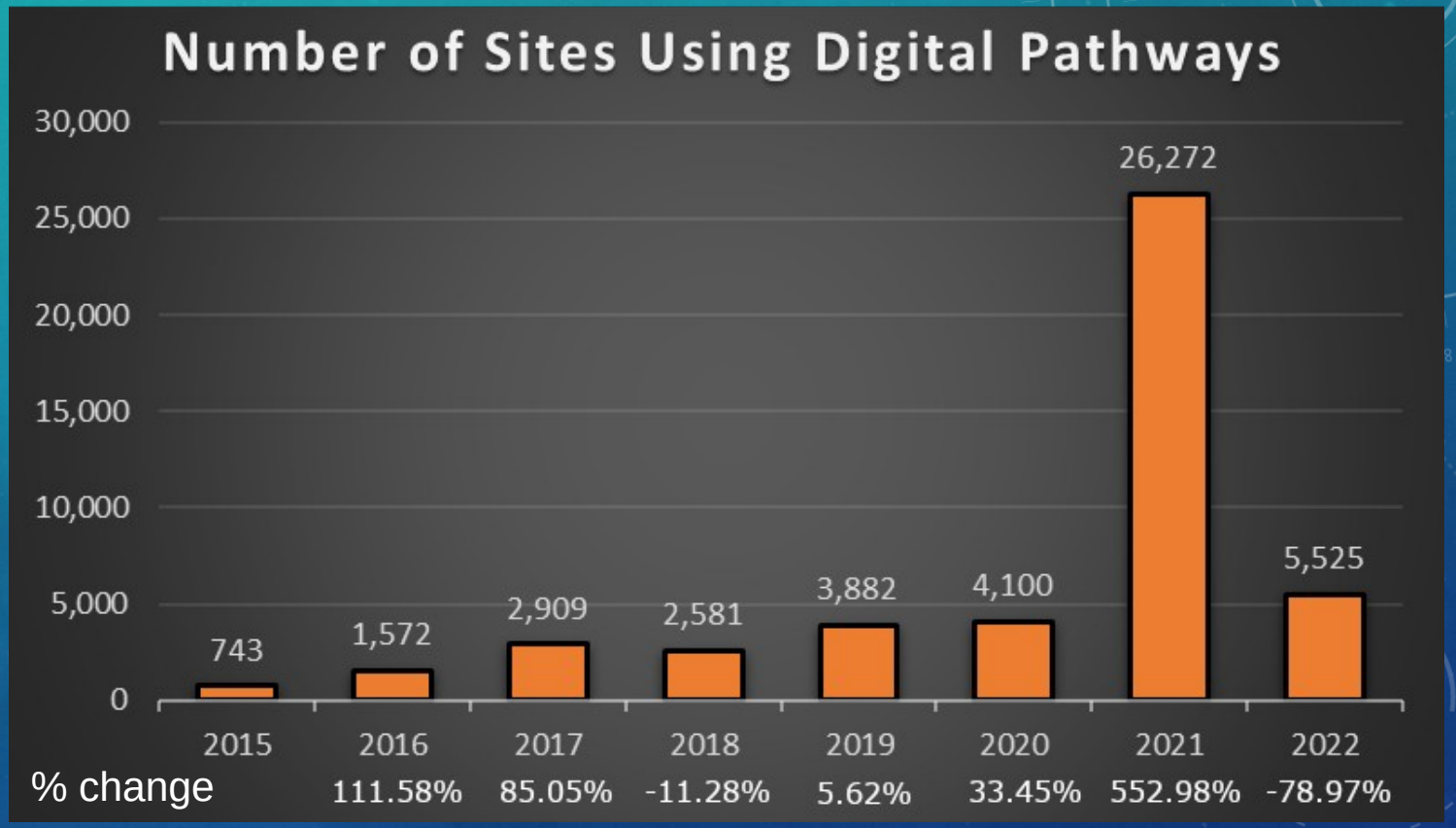
Digital Pathways

- Following a set path of multiple links to show malicious content
- This is identical to the friendly referrer / friendly intermediary examples
  - 5525 sites using this countermeasure were identified by the IWF in 2022
- Must follow the set path in order to gain access to content.



Digital Pathways

- Monitored by IWF since 2011
- Chart shows number of sites using digital pathways found by IWF and the percent change from previous year
- 4,100 sites in 2020
- 26,272 sites in 2021
- 5,525 sites in 2022



Content Obfuscation

- Content obfuscation could be done by changing the content itself
  - encryption, stenography, etc
- Not supported by this Meta Analysis from Edinburgh University published in Forensic Science International: Digital Investigation
  - “About 7% of content was encrypted by offenders until the inclusion of default encryption”
  - ~1% in 2006 used stenography
- Dynamically changing the content of their website based on some criteria
  - Geolocation
  - The use of some “obscure token”
- The Demo focuses on the idea of an “obscure token”

OBSCURE TOKENS DEMO

Obscure Tokens

- An obscure token is some piece of information that is hard to guess but is necessary to revealing the hidden content
- Adversaries could use this obscure token in order to hide the malicious content with a simple
- if(user_has_obscure_token): show_bad_content()

  else: show_Good_content()
- How might an adversary use an obscure token?

Methods for Using Obscure Tokens

- I have identified 5 ways that they could possibly do this
- Friendly Referrer links
  - If user came from a friendly website, show them the malicious content
  - Possibly necessary for digital pathways
- Cookies
- Session token
- Logging into a different website (though this one is known)
  - If user is logged into website x show them malicious content on website y
- There are pros and cons to all of these methods.
- Demo shows bare minimum to accomplish these techniques.

Technical Setup for demo

- Dnsmaq for DNS
- Nginx for reverse proxy
- Jinja Templates and Python3 Flask
  - Front and back end
- Docker for convenience.
- Make for extra convenience.

NGINX

Jinja

python™

docker

First Page: an innocuous cat blog

- Navigating the demo website reveals little about the site itself, it appears to be an ordinary cat blog…
- Or is it?


WHAT IF I TOLD YOU
THIS WAS NOT A BLOG ABOUT CATS
imgflip.com

Second Page: a malicious website.

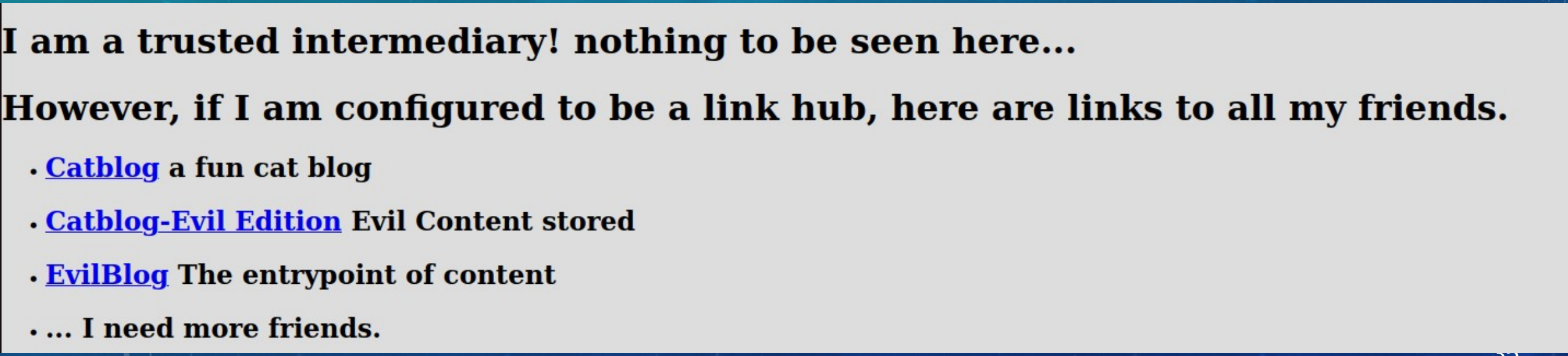
- This website is the gateway to any malicious content stored.
- Responsible for giving the user the Obscure Token in a variety of ways.
- This secondary page may either be disguised or dubious, depending on the craftiness of the adversary.

Friendly Referrers

- If the user clicks the Friendly Referrer link, they will be redirected back to the catblog.
- Catblog sees this and shows malicious content, because the link came from a “friendly” website.
- Main Pro: unable to be found without first discovering the second site.
- Main Con: requires a certain degree of trust.
  - Digital Pathways resolve this to a certain extent.

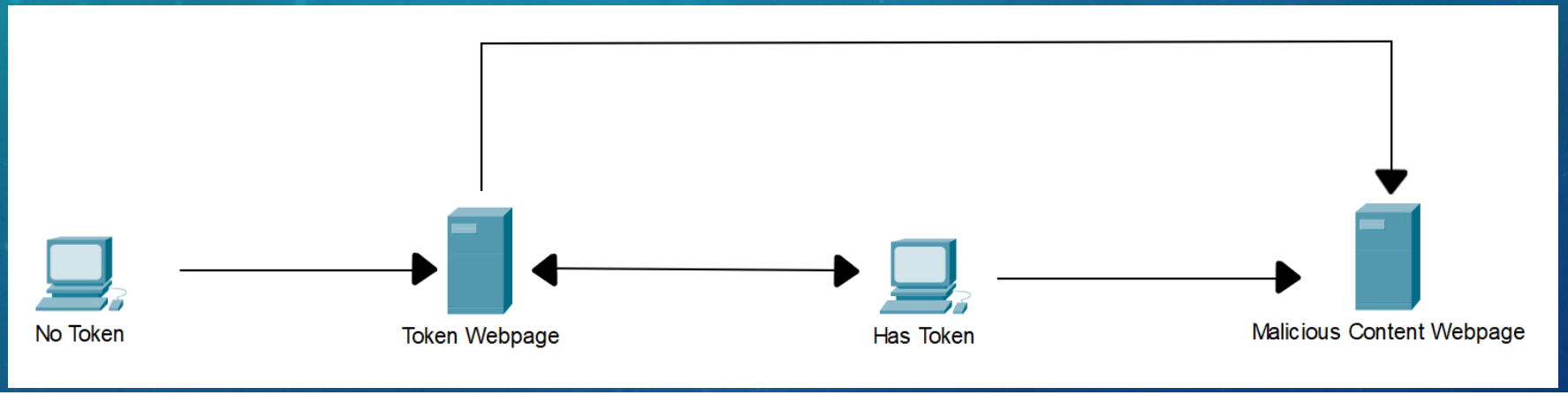
Friendly Intermediaries

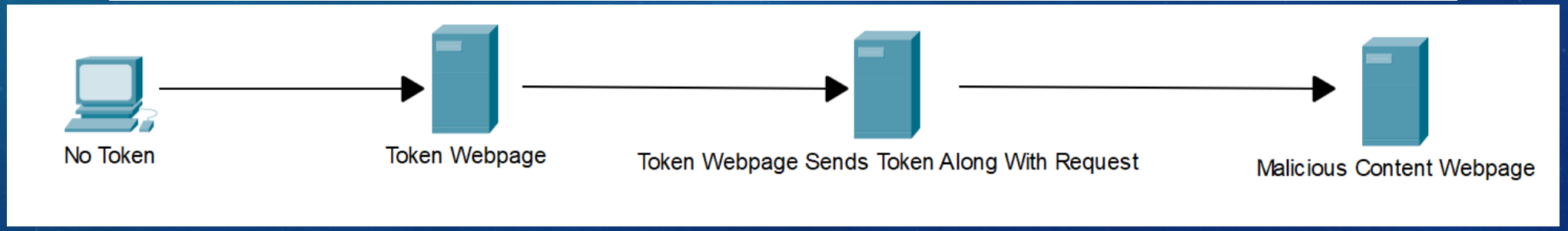
- Handle the exchange of the tokens between websites
- Cuts out trusting everyone, instead trust only one
  - More malicious websites can share links to other malicious websites
- Can also serve as a “Link Hub” hosting links to all malicious websites, if you happen to find it



Token as part of the server/client

- Token is given to the user as a part of either the client (given on the evil web-page itself) or the server (on request)
- The user is then redirected to the catblog and is shown content



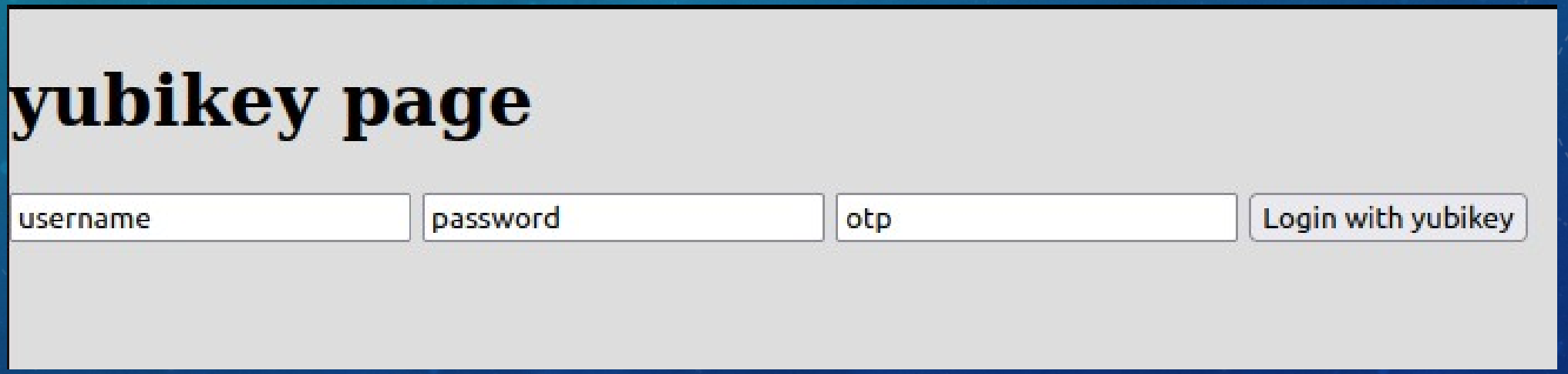


Other Website Login

- Not new
- Can use Cookies / Universal Login / SSO to log into multiple websites at once
- Put simply: if user logged into evil_site show malicious content on hidden site.

Hardware Token

- This obscure token could also be a “hardware” token, like a Yubikey.
- Hardware tokens simply provide another layer of security
  - Can be used for 2FA
- An adversary could sell these tokens and this is how they use it to log in.

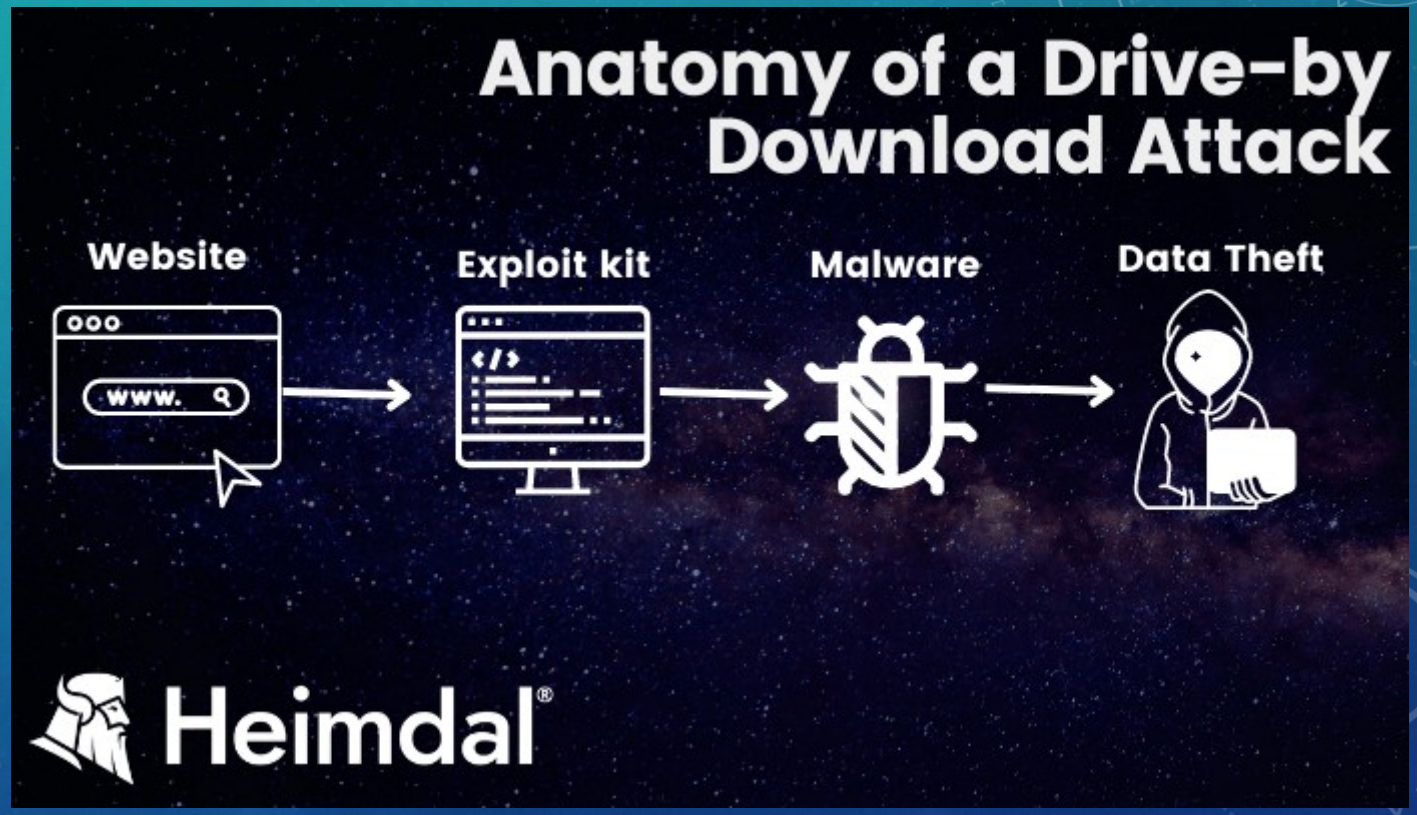


What else can you do with this (bad)?

- Send people a malicious link that refers back to your own web server to infect machines.
  - http://cat.blog.com/totalySafeLink
- Can be targeted as necessary. (wider rate spear phishing)
  - IP address, cookies, other identifying information.
- Host a “catch all evil business” like the Silk Road.

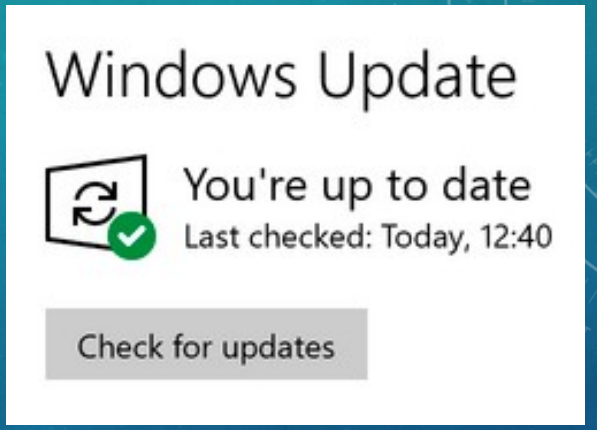
Drive By Downloads

- Files that automatically download without your knowledge or concent
- These programs can be used at the time of download for malicious purposes, or they may lie dormant until later.



Protections

- Keep your computer up to date
  - Including web-browser and OS
- Verify download source
- Don’t use unnecessary or outdated plugins (Flash)
- Anti virus programs can catch this in action and help prevent infection.
- Traffic Filtering



What else can you do with this?

- Show two different versions of the same news story
  - Show the “CCP approved” version if the user’s IP comes from china, show a “different” version if they originate elsewhere
  - Republican vs Democrat
- Is it ethical or moral to do so?

Detection and remediation.

- Now that we know this is plausible, how do we find it and put a stop to it?
- Well… we can’t
- If website is known:
  - brute force the obscure token, friendly referrer, capture session token
  - Possible, depending on how the obscure token was generated, how it is used, and how good their security is.
- If website is not known:
  - Visit every website from every other hoping to be given a token: NOT COMPUTABLE
  - Infiltration via law enforcement
- There may be a better, more clever solution out there, but I could not come up with one.

Did I find any example of this being used?

- I could not find any example of this being used.
- This is a job for the FBI anyway.

Design Metrics

- Reachability
  - How many users can this content reach?
  - Higher score means more users are reachable
- Detectability
  - How easy is this to find?
  - Higher Score means it is easier to detect
- Security
  - How secure is the content?
  - Higher Score means it is more secure or has more security measures in place

Adversarial Goal

- Maximize reachability and Security while Minimizing how detectable it is

Scoring Primer

- Score is x/10
- An arbitrary metric that feels appropriate
- not based on math or statistics.

Conclusion

		Reachability	Detectability	Security
Social Networks	Large Social Network	8	8	2
	Federated Mastodon	5	6	3
	Unfederated Mastodon	2	2	5
Encrypted Telecommunications		2	0 or 10	8
Tor		3	3	8
Usenets		3	7	3
Torrents		6	7	2
Digital Pathways		4	3	8
Obscure Tokens		7	1	9

Social Media Chart

Tor Study

OCRS 2022 Presentation

Hosting Providers Study

Github Demo Code

Scores

Social Networks

- Reachability:
  - Large social network – Large visibility
- Detectability:
  - Content moderation teams
  - Large amount of nonmalicious content makes it more difficult to find
- Security:
  - Fake accounts
- Each category is dependent on the Social Network used

Encrypted Telecommunications

- Reachability:
  - Depends If it was posted publicly or not
- Detectability:
  - If one member is law enforcement: 100% detectable.
  - If both are adversarial: 0% without a warrant. (see Security section)
- Security:
  - Depends on the specific app, no app is without security flaws.
  - Information obtained by law enforcement is dependent on what app is used and what other security measures are in place.

Tor

- Reachability:
  - Difficult search engine indexing
  - Users must connect to the Tor network
- Detectability:
  - Must be on the Tor Network to access hidden services
  - Tor network traffic is pretty easily identifiable
- Security:
  - There are a variety of techniques that can be carried out against the Tor network.

Usenets and Torrents

- Considerations:
  - Requires use of a program and/or signing up for a service
- Reachability:
  - Only reachable to people on Usenet / torrent
- Detectability:
  - Could be found fairly simply if you know what to look for
- Security:
  - Usenet is an obscure service (these days)

Obscure Token

- Reachability:
  - Website is hosted in clear web, but you have to find / be given the token
- Detectability:
  - Undetectable without the token
    - except in the case of friendly referrers / digital pathways
  - Not Computable
- Security:
  - Depends on the method used and the security of the website itself

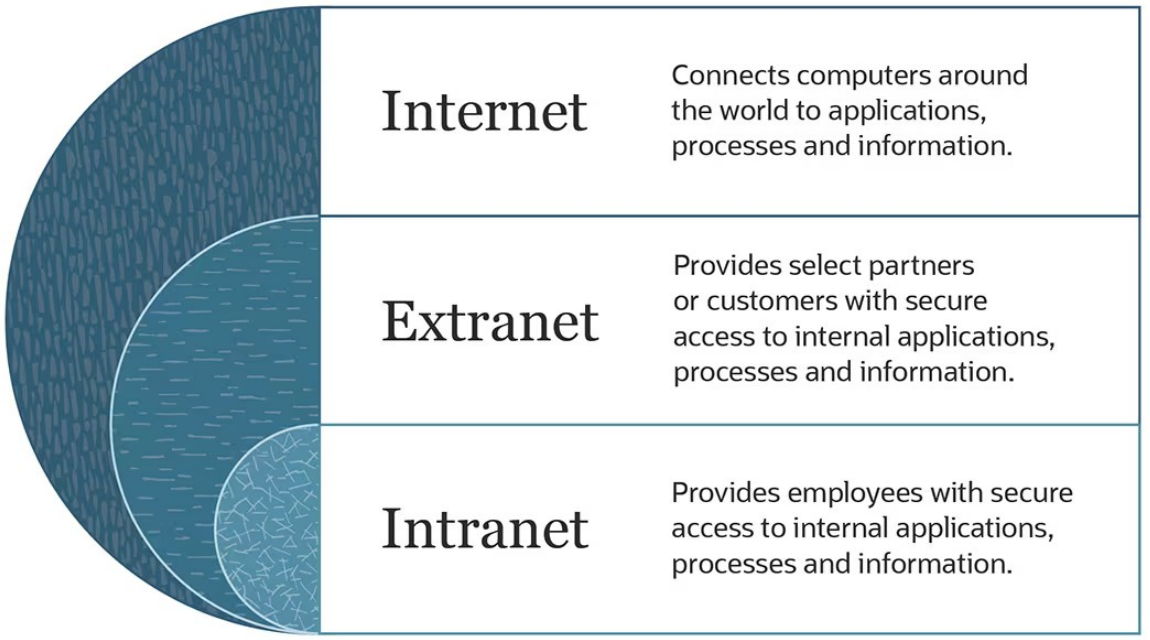
Extras

Encrypted Web Traffic VPNs

- Similar to Tor, adversaries can use a VPN to encrypt their web traffic
- Used for good reasons and bad
  - Privacy
  - Additional layer of encryption protects individual from AiTM snooping
- Instead of trusting your ISP to not snoop, you're trusting a 3rd party instead
- A better application for VPNs is a private intra/extranet

Malicious private networks and Usenets

- Instead of using Tor adversaries could use private intra/extranets to hide their malicious content.
- Limits access to other adversaries who have been granted access



Internet, extranet and intranet core differences.

Hardware Encryption Keys

- Another Idea is that the adversaries offer some/all their content, albeit encrypted, for free
- In order to access, you must purchase the encryption keys in order to gain access to whatever content they have
- This could be as simple as running your own decryption software with the provided keys
- Or the encryption keys and software are sold on the same device

Expanded Information

Aspects of adversaries and malicious content

	Advertising	Communication	Storage	Transmission
Social Networks	X	X	X	X
Encrypted Web Traffic				X
Encrypted Communication		X	X	X
Torrents			X	X
Usenets	X	X	X	X

Aspects of adversaries and malicious content

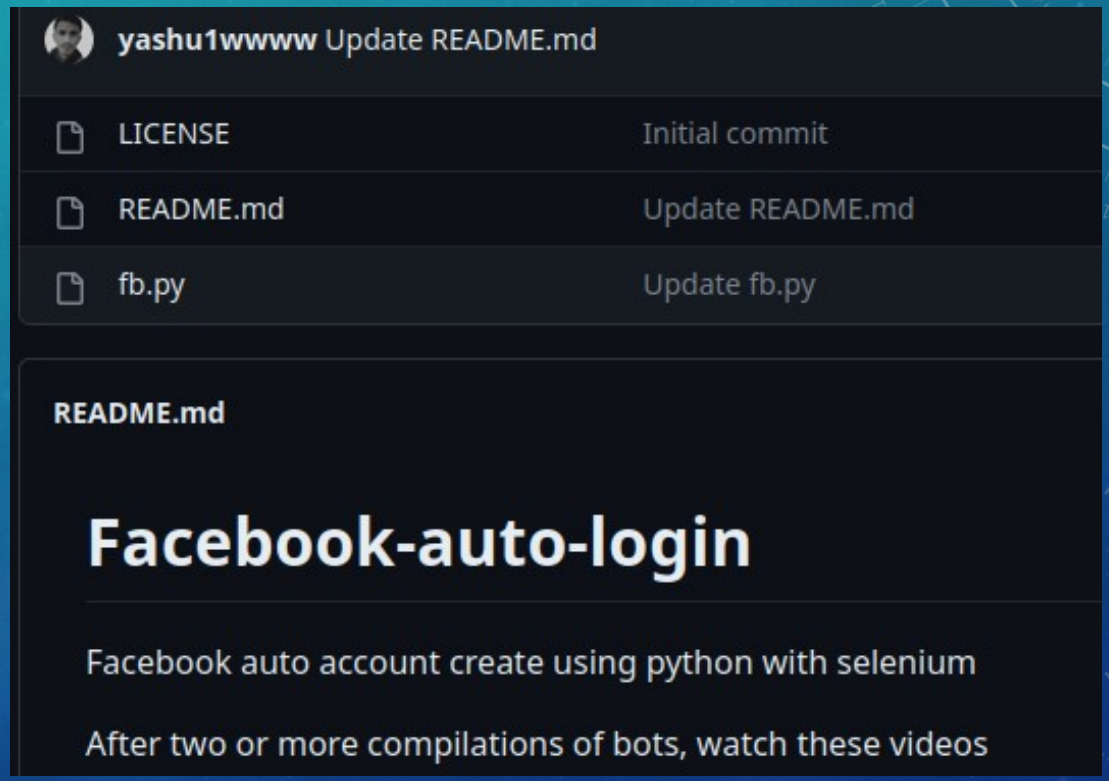
	Advertising	Communication	Storage	Transmission
Social Networks	X	X	X	X
Encrypted Web Traffic	X			X
Encrypted Communication	X	X	X	X
Torrents	X		X	X
Usenets	X	X	X	X

Communication

- Communicate between buyer and purchaser or between two swappers
  - Swappers swap malicious content instead of buying and selling it
- May post their contact information in some public capacity (e.g. on social media)
- Storage
  - Local
    - Phone, computer, external storage device
  - Website / Hosting server
    - Have someone else host the content for you
- Transmission via
  - TCP / NNTP / FTP / in person

How adversaries use social media

- Fake accounts
  - Makes it more difficult to track
  - Easy setup with automation
  - Enable all behavior below
- Scamming
- Communication
- Uploading content to social media company

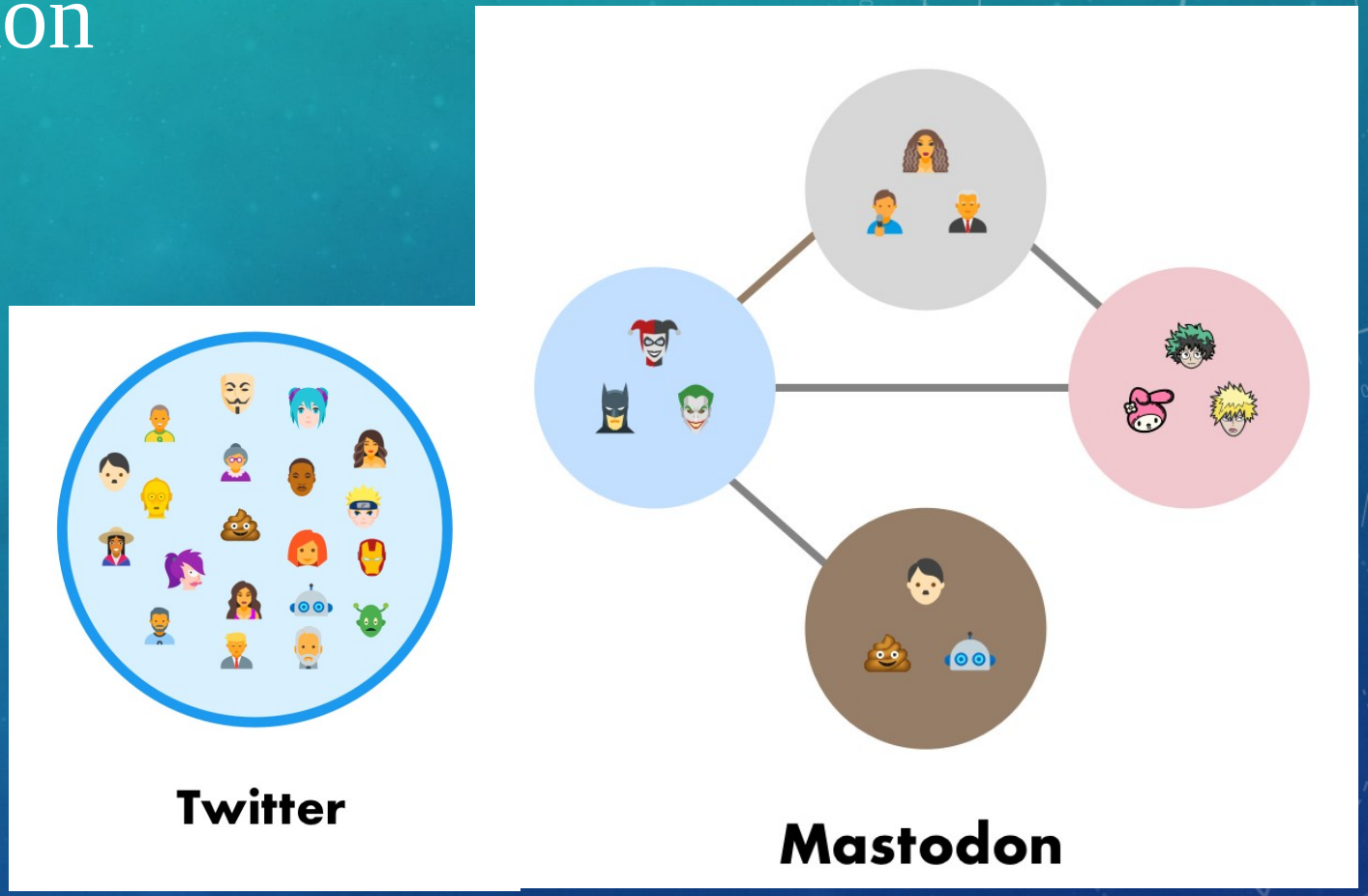


Social Networks - Mastodon

- Mastodon is a social network framework of sorts
- Content is moderated by the site itself, no central team like in Facebook or Twitter.
- Instances are much smaller than Facebook and Twitter, often being focused on one specific group (I.E. https://infosec.exchange/)
- This allows for smaller, more focused, social media instancies

Social Networks - Mastodon

- Can link with other Mastodon instances through “Federation”
- User’s posts on Federated instances are shown to members on the other instance
- Can also De-Federate instances
- Defederated instance’s content does not shows up in the site that defederated it



Social Networks - Mastodon

- Smaller size is both a good, and a bad thing
  - Better more focused information
  - Echo chambers
- Private closed mastodon instance

Social Networks – Use Case

- Could be used for adversaries to connect with one another
- Limited “advertising” of their site/content
- Used mostly for connecting / exchanging information, rather than malicious content itself
- More likely to be found by content moderators

Social Networks

- Content moderation teams should work with law enforcement
  - Report any suspicious behavior
- Automatic content moderation via blocklisting certain tags

Encrypted Telecommunications

- Require a certain degree of trust that the person on the other end is another adversary
- Requires both parties to have the same app
- Requires that one party know the other's contact information
- Posting contact info in some public capacity leaves a higher likelihood of detection

Encrypted Telecommunications

- Law enforcement agencies are the best equipped to handle this
- Can setup a sting to capture individuals once malicious information has been found
- Work with the app creator to ban accounts of abusers
- Administrators
  - Ban users ‘advertising’ malicious content or contact information

Usenets vs Torrents

Usenets:

- Speed uses maximum bandwidth specified by provider
- Multiple single “whole file” sources
- Use NNTP (Network News Transfer Protocol)
  - Allows both client/server and server/server communication

Torrents:

- Speed depends on number of seeds.
- Multiple “partial file” sources (seeds)
- Use P2P (Peer to Peer)

- Both Allow for the sharing of copyrighted material, may host viruses and other such malicious content

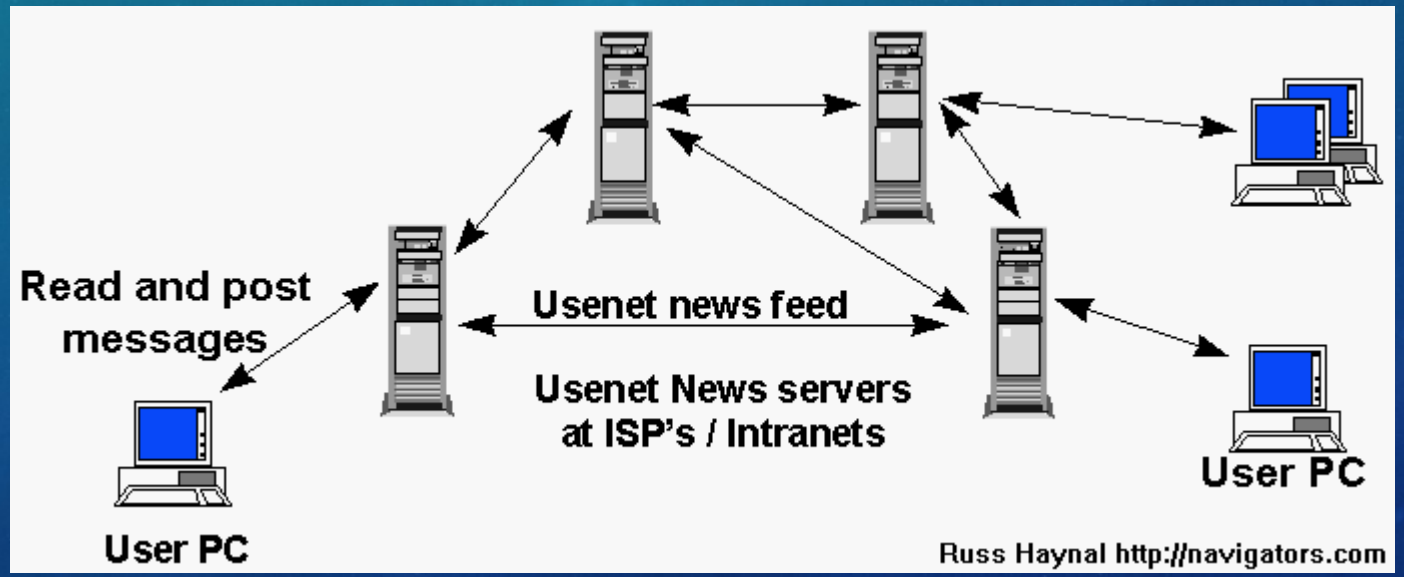
Usenet

Benefits

- Timed life of uploaded content
- SSL Encryption
- Not widely known
- Many providers do not keep activity logs

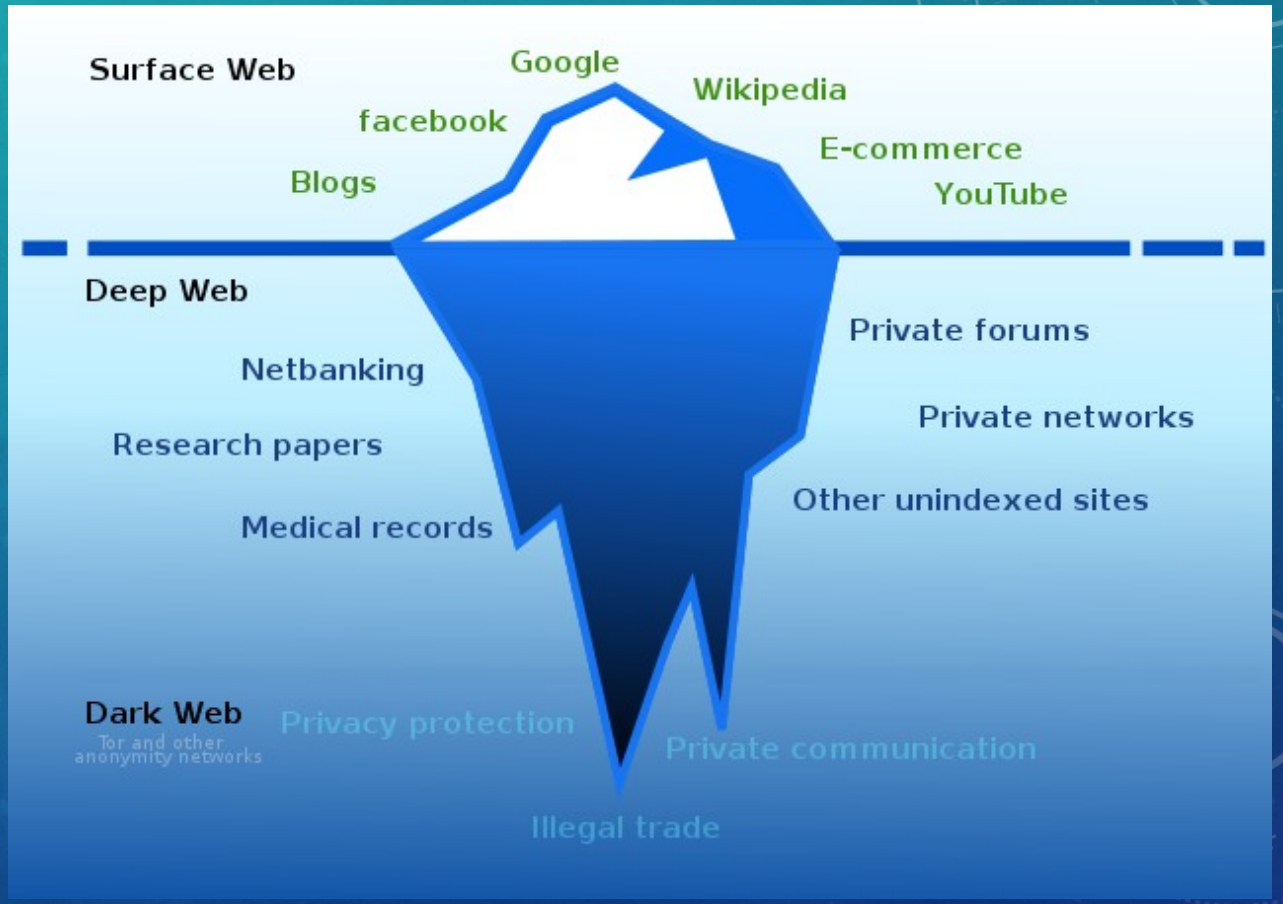
Drawbacks

- Have to pay a Usenet provider, making it more difficult to remain anonymous.
- Many providers have Capped data plans



Clear Web Websites

- Websites hosted in the Clear web (normal internet) have the greatest potential reach
- Are accessible by anyone who knows (or is given) the URL
- Able to use search engines to find the site
- Widely Accessible
- This is also the problem
  - Because anyone who visits can see it, it is much more likely to be taken down
- How do adversaries maximize their reach while also not getting caught?



Garbage URLs

- Using a nonsense url (E.G. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) makes it harder to find than human readable ones (E.G. stop-wanna-cry-now.com)
- Lower ranking on search engines
- Higher security, Lower Detectability and Reach

xkcd.com/1247

Fingerprinting

- Facebook and Twitter, (see also Google Ads) use something called Fingerprinting
- Similar to how fingerprints on humans are ‘unique’ the practice of fingerprinting serves to identify users through their own browser
- Collects information about browser/OS, microphone/camera, fonts, plugins, etc.
- You can see your fingerprint using the website https://amiunique.org/
- The idea is to serve content and ads more personalized to the user currently on the website
- Could this be exploited for malicious purposes?

What if the obscure token was a fingerprint?

- Adversaries engaging in similar activities probably have similar browser fingerprints*.
- Now if you advertise this to the world on the clear web, it still requires a fingerprint or cookies to match.

- *Assuming they don’t clear it out or manipulate it.

Extension

- Could we then build a toolkit to Opt-In websites to this sort of fingerprinting or obscure token analogy?
- I see no reason why not.