

Wild Wild Phish: Phrontiers in the Phight Against Phishing

Adam Doupé

Associate Professor

School of Computing, Informatics, and
Decision Systems Engineering



GNU Operating System - Free Software Foundation



[Free as in Freedom](#)

Welcome to the GNU Project web server, www.gnu.org. The [GNU Project](#) was launched in 1984 to develop a complete UNIX style operating system which is [free software](#): the GNU system. (GNU is a recursive acronym for "GNU's Not UNIX"; it is pronounced "guh-noo.") Variants of the GNU operating system, which use the kernel Linux, are now widely used; though these systems are often referred to as "Linux," they are more accurately called [GNU/Linux systems](#).

This is also the web site of the [Free Software Foundation](#) (FSF). FSF is the principal organizational sponsor of the GNU Project. FSF receives very little funding from corporations or grant-making foundations. We rely on support from individuals like you who support FSF's mission to preserve, protect and promote the freedom to use, study, copy, modify, and redistribute computer software, and to defend the rights of Free

WorldWideWeb	Style	Document	Navigate	Find
Info	Copy style	Open file...	Back	Find Panel...
Navigate	Apply style	Open given document address	Next	Find Next
Document	Address	New file...	Previous	Find Previous
Find	Lists	Respond	Home	Enter Selection
Edit	Glossary	Save	Panel...	Jump to Selection
Links	Example	Save all edited windows	Links	
Style	Normal	Save a copy in	Mark all	
Print...	Heading 1	Inspect ...	Mark selection	
Page layout...	Heading 2	Diagnostics)	Link to marked	
Windows	Heading 3	Miniaturize	Link to New	
Services	Heading 4	Open master template document	Unlink	
Hide	Format	Close all other windows	Link to file...	
Quit	Panel...	Close	Help	

HyperMedia Browser/Editor

Version:

2.02 with libwww 2.16pre 1

exercise in global information availability
original WorldWideWeb program

by Tim Berners-Lee

Copyright 1990,91,93,94, TBL, CERN. Distribution restricted: ask for terms.

Text: Text which is not constrained to be linear.
Media: Information which is not constrained linear... or to be text.

This is a new version of the NextStep WorldWideWeb application with the libWWW library. Bug reports to timbl@info.cern.ch, quoting the version information above. Check the list of known bugs in the web too.

This was the original prototype for the World-Wide Web. Many browsers for other platforms now exist (Read the web for details). After many years lying fallow, this application has now sprouted images and nested HTML elements and things. If you have an Internet connection, then using "Help" under the Info menu will tell you all about this application. If you don't have an internet connection -- get one! ;)

If you want to be able to read news, you should set the name of your local news server in the preferences.

Mark/Inspect

Selection Link destination Image

Change

Link selection to marked Insert image

relationship (none)

Marked:

Address:

Open







Dialing...



Main Help

AOL Chat Room Listings

Search All Chats by Topic:

Chat With People Like You

- [Piercing and Tattoos](#)
- [Elvis Sightings](#) | [Britney Fans](#)
- [Disquads](#) | [My Girlfriend](#)

Created by People Connection

Created by AOL Members

1 Double-click to choose a category:

Category
Town Square
Arts and Entertainment
Black Voices
Friends
Gay & Lesbian
Latino
Life
News, Sports & Finance
Places
Romance
Special Interests

2 Double-click to enter a room:

People	Rooms in "Town Square"
36	The Bonfire
1	A Chill in the Air
35	A Crowded Room
1	Beach Party
1	Best Lil Chathouse
35	Biker Bar
36	Bored
1	Break Time
10	The Breakfast Club
25	Friends of BMW

- Start Your Own Chat
- Enter or Start Private Chat

Top City Chats

1. [New York](#)
2. [Los Angeles](#)
3. [Miami](#)
4. [Chicago](#)
5. [Boston](#)

Go Where the People Are



Rate photos, flirt a little, get the star treatment, more:
 • [Join the Fun](#)

starring in alphabetical order

GEORGE CLOONEY MATT DAMON ANDY GARCIA BRAD PITT and JULIA ROBERTS

OCEAN'S ELEVEN



WILLIAMS PICTURES PRESENTS
A WOLFGANG PETERSEN FILM
GEORGE CLOONEY MATT DAMON
ANDY GARCIA BRAD PITT and JULIA ROBERTS
"OCEAN'S ELEVEN"
CASTING BY JEFFREY KURLAND
EDITED BY CARL BEVIER
PRODUCTION DESIGNER PHILIP MESSINA
EXECUTIVE PRODUCERS PHILIP MESSINA DAVID FOLLOWS
PRODUCED BY JERRY WEINSTEIN
SCREENPLAY BY JOHN DAHLER
DIRECTED BY WOLFGANG PETERSEN

Own it on Video and DVD



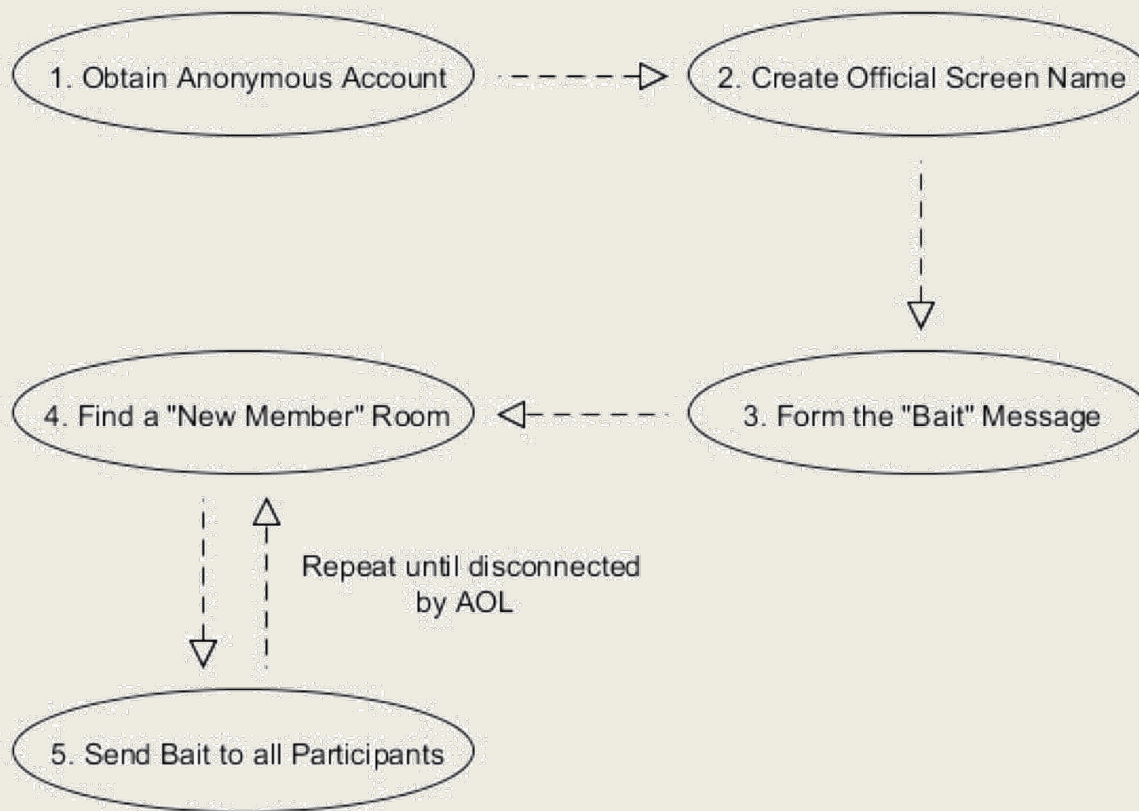


Figure 1: Password and Credit Card Scam Process



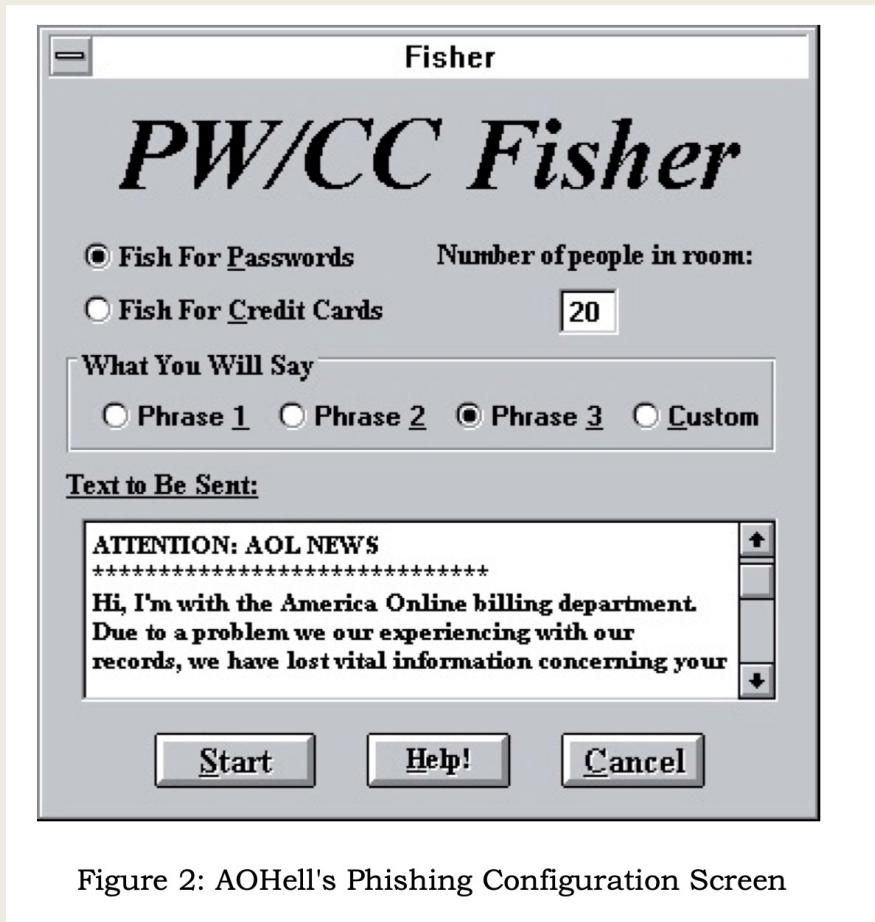


Figure 2: AOHell's Phishing Configuration Screen

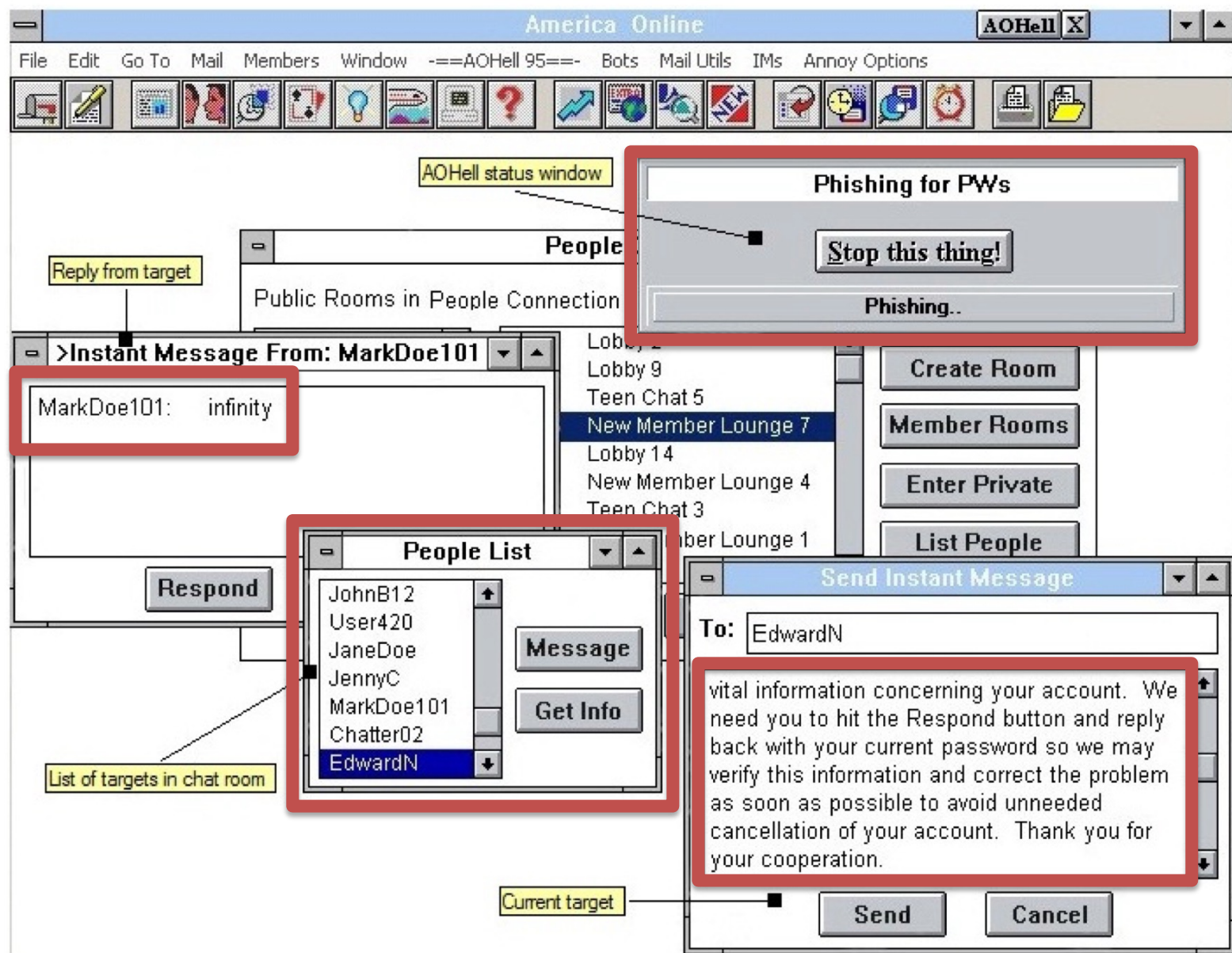


Figure 3: Automated Phisher in action on Windows 3.1 and AOL 1.1



AMERICAN EXPRESS

Dear Customer,

You have an important notification on your Card

Your access to americanexpress.com has been temporarily restricted because of suspicious activity that was detected on your Card.

Please take time to sign on to your account immediately to review your recent account activity.

[Sign On to Security Center](#)

We apologize for any inconvenience and appreciate your understanding.

Thank you for your Card Membership,

American Express Customer Care

DON'T *live life* **WITHOUT IT™**

[PRIVACY STATEMENT](#) | [UPDATE YOUR EMAIL](#)



[My Account](#) [Cards](#) [Travel](#) [Rewards](#) [Business](#)



[Help](#)

[Log In](#)

USER ID

PASSWORD

Cards - My Account



Remember Me

[Log In](#)

[Forgot User ID or Password?](#)

[Create New Online Account](#)

[Confirm Card Received](#)

[Visit Our Security Center](#)

FROM OUR PARTNERS



ABOUT

[About American Express](#)

[Investor Relations](#)

[Careers](#)

[Site Map](#)

[Contact Us](#)

PRODUCTS & SERVICES

[Credit Cards](#)

[Small Business Credit Cards](#)

[Corporate Cards](#)

[Prepaid Cards](#)

[Savings Accounts & CDs](#)

[Gift Cards](#)

LINKS YOU MAY LIKE

[Membership Rewards](#)

[Free Credit Score & Report](#)

[Credit Secure](#)

[Bluebird](#)

[Accept Amex Cards](#)

[Refer A Friend](#)

ADDITIONAL INFORMATION

[Card Agreements](#)

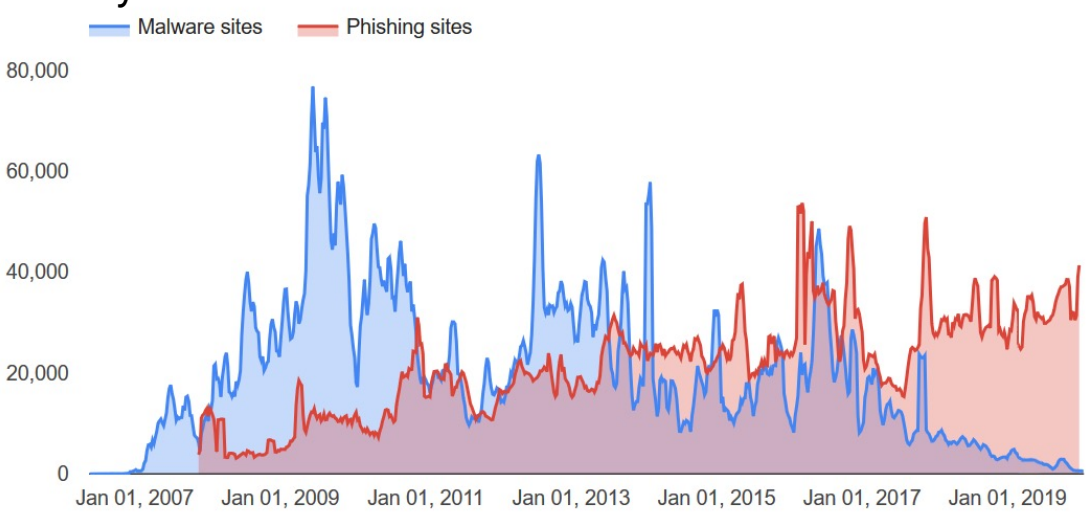
[Financial Education](#)

[Servicemember Benefits](#)

[Supplier Management](#)



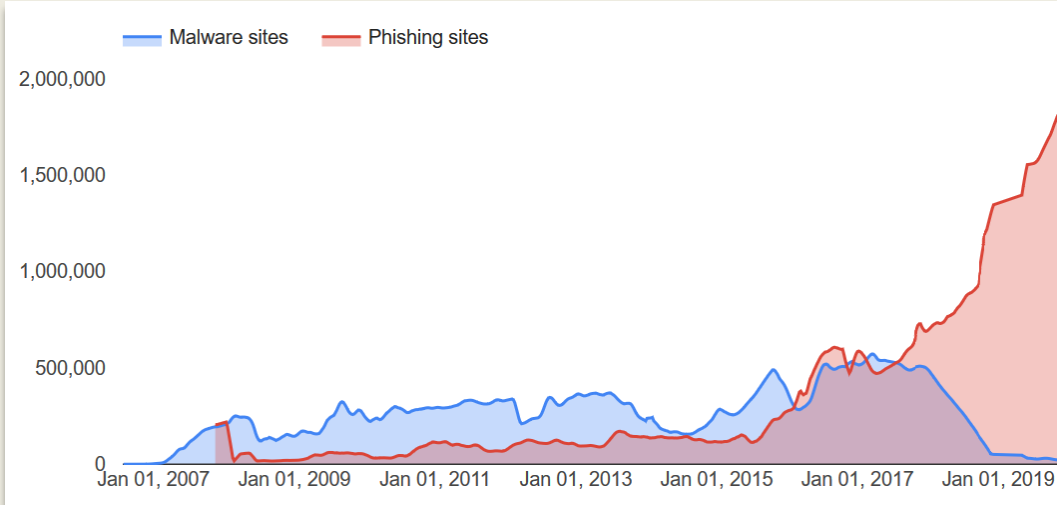
Weekly Malicious Site Detections [1]



Phishing

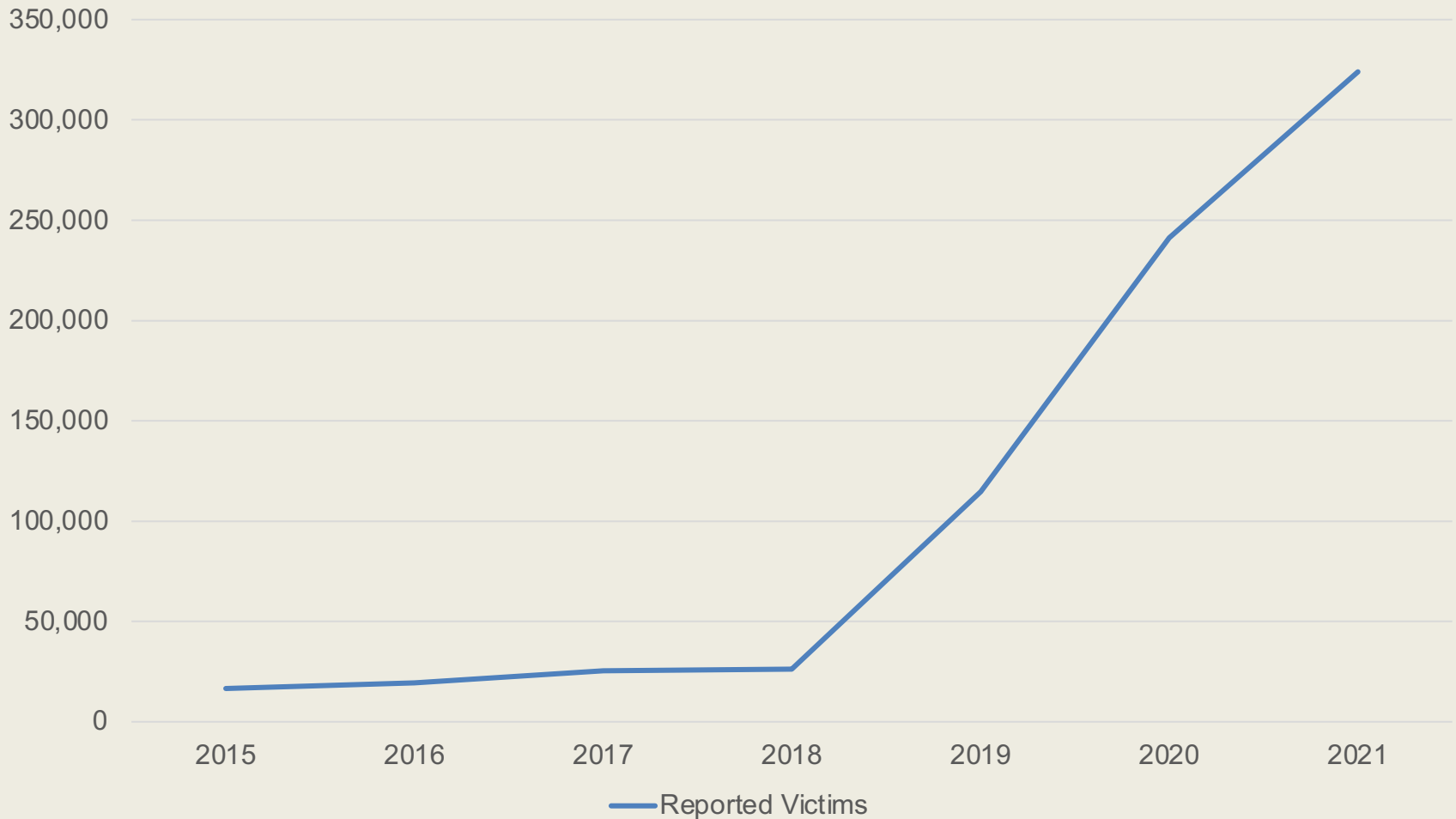
Web-based malware

Total Malicious Sites Online



[1] Google Safe Browsing Transparency Report: <https://transparencyreport.google.com/safe-browsing/overview>

FBI I3C Reported Phishing Victims Per Year



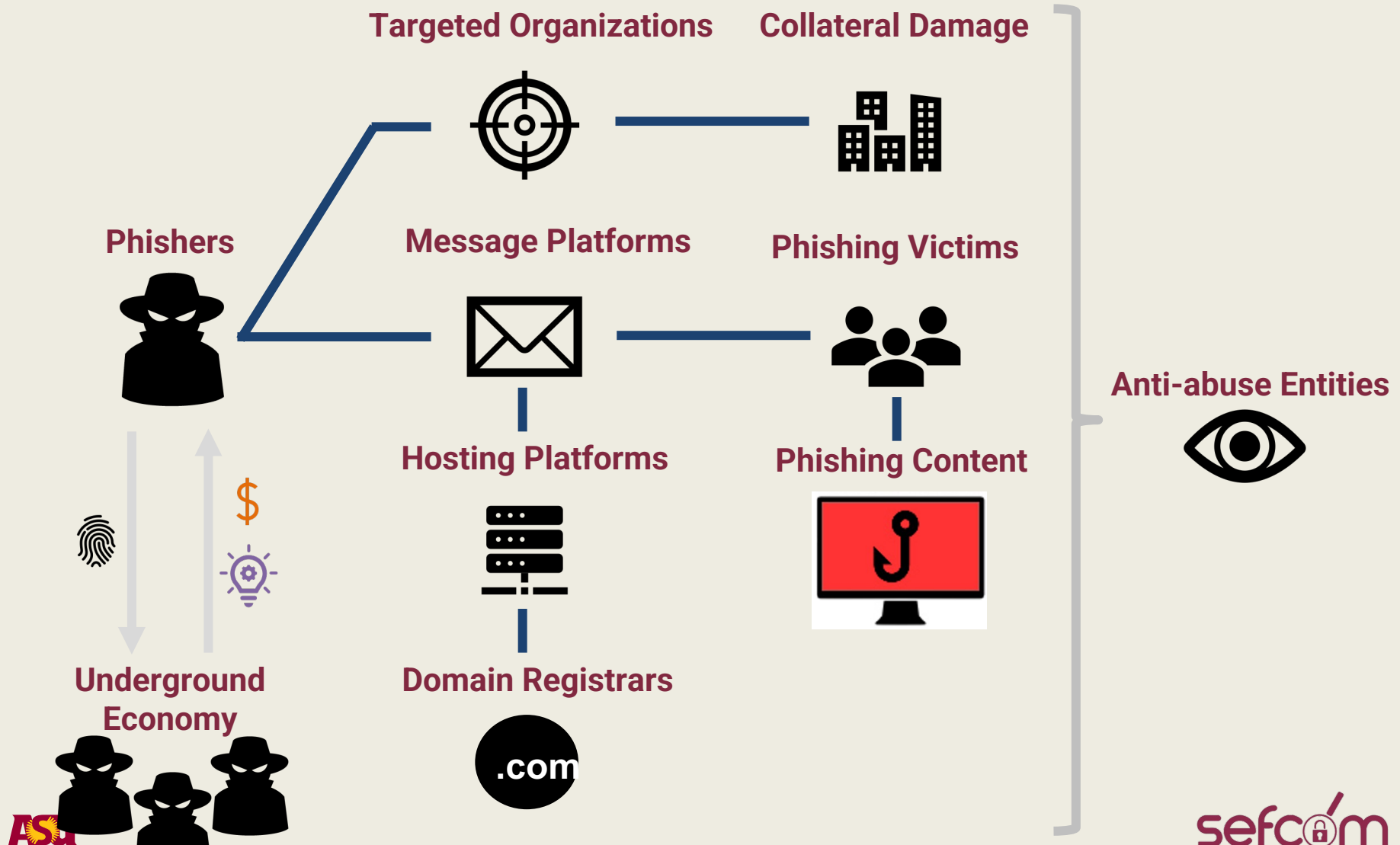
Likely undercount according to Breen et al., "A Large-Scale Measurement of Cybercrime Against Individuals" CHI 2022.



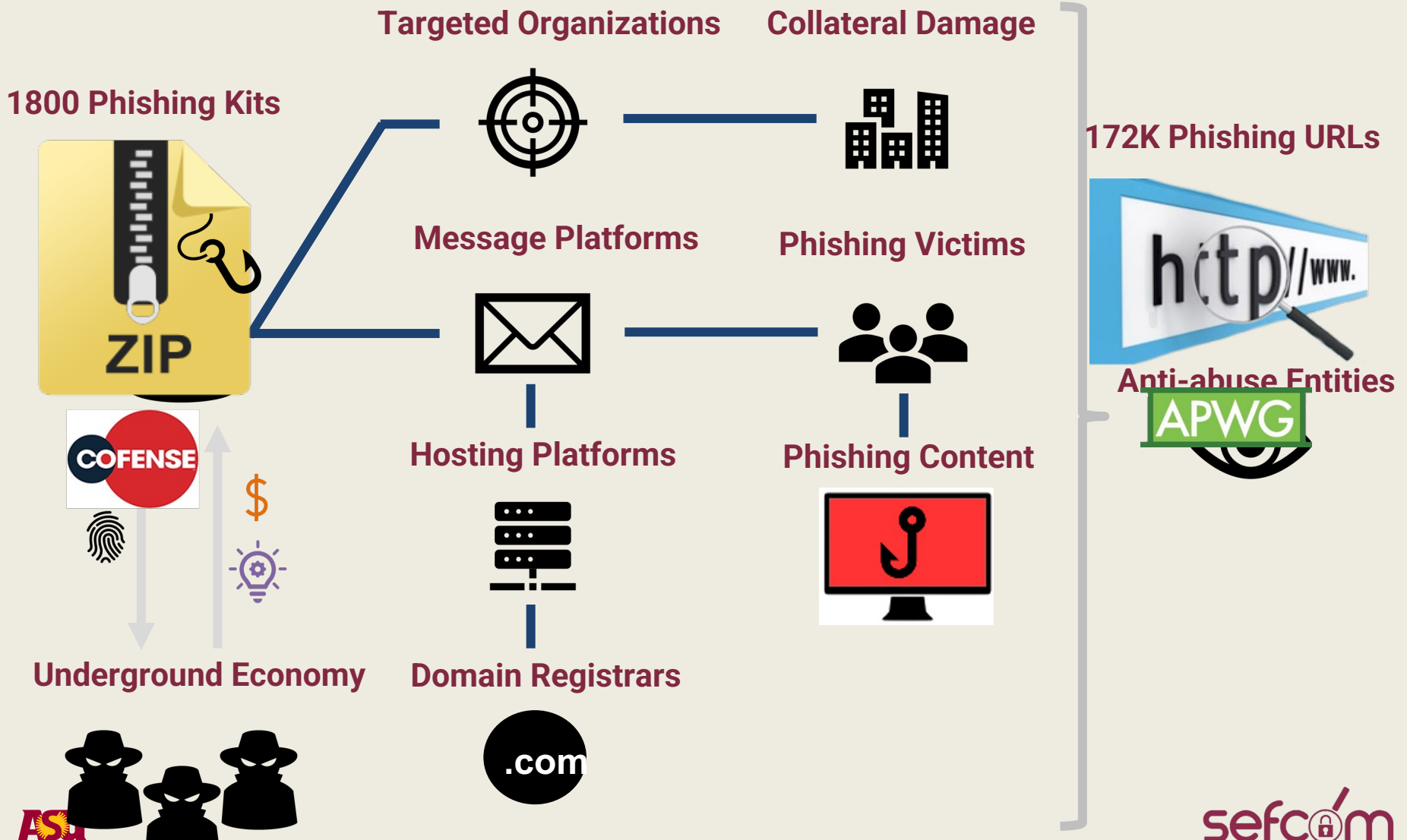
Phishing Questions

- Why does phishing continue at scale?
- What shortcomings exist within anti-phishing systems?
- How can we reliably measure them?
- How can they be improved?

Anti-phishing Ecosystem



Digging Deeper



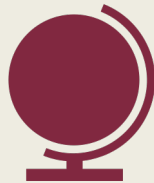


Phishing Kit Analysis

- 2,300 *.htaccess* files
 - Used heavily to block security organizations
 - 1.5M total directives, 340K unique



Hostname/IP



Geolocation



User Agent



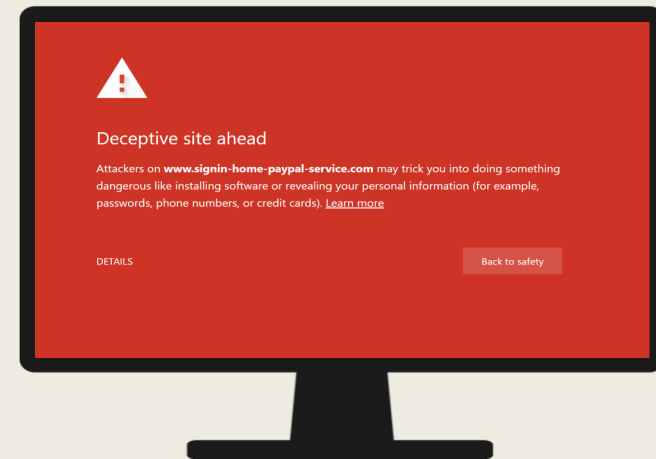
Referring URL

Why is request filtering so elaborate?

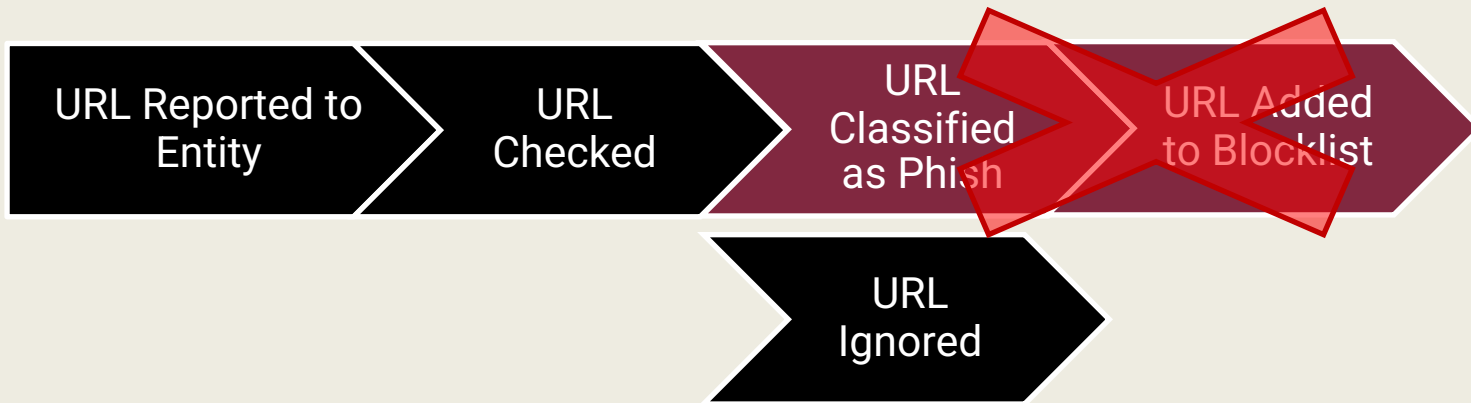
Do phishers truly understand the ecosystem?

Anti-phishing Blocklists

- **Key ecosystem defense**
 - Default in major desktop + mobile browsers
 - App and e-mail integration
- **Goals**
 - Timely, comprehensive detection
 - Low false positive rate
- **Automated crawler backend**



“Cloaking”: Why Filter Requests?



Attack stays online longer: phishers **maximize ROI**

Can current anti-phishing systems **bypass cloaking**?



HOW TO MEASURE A FISH

MEASURE THE FISH WITH MOUTH CLOSED AND TAIL FIN COMPRESSED TO DETERMINE TOTAL LENGTH.



PhishFarm Research Overview



Do **browser blocklists** protect users from cloaked phishing?

- **Coverage:** does blocking always occur?



- **Speed:** lag time before blocking happens



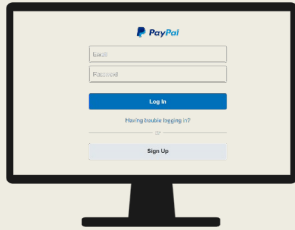
- **Consistency** across platforms



Security implications of gaps?

Measuring Blocklists

- **Framework to create** our own harmless phishing sites



- **Preliminary experiments** to guide design of larger ones (cloaking, entities, URL types)



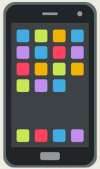
- **Preliminary security recommendations**



5 Cloaking Techniques



A. Allow **all traffic** (control group)



B. Only **mobile** (Android & iOS)



C. Only **US** desktop

D. Only **non-US** desktop



E. “**Anti-crawler**” IP/hostnames (from *.htaccess*)

JavaScript

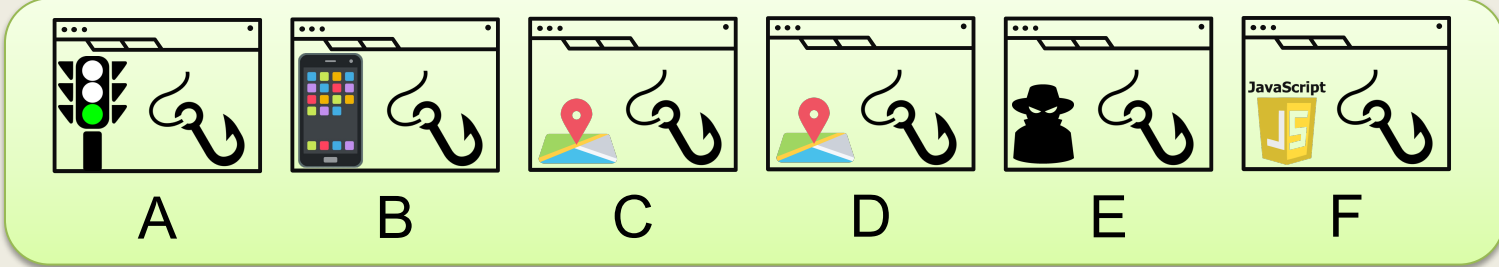


F. Only if **JavaScript** runs in browser





Full Experiments



x 66
= 396 sites

x

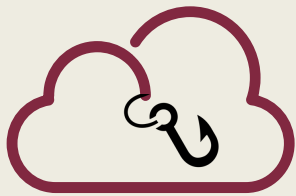


= 1,980 sites total

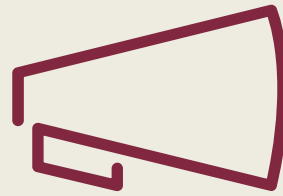
Random .com domains (avoid confounding effects)



PhishFarm Deployment



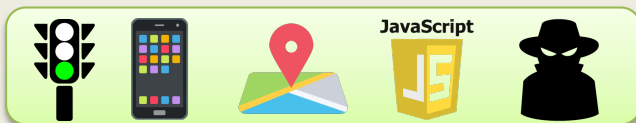
Configure & Deploy
Phishing Sites



Report URLs to
Anti-Phishing Entities




Monitor Browser
Blocklist Status
(desktop + mobile)



1 hour of setup
End-to-end automation

Overview of Findings

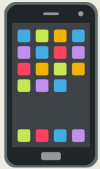
- Over 2M web hits, 20K blacklist timestamps
- Cloaking **halved blocklisting** chance, nearly **doubled time** to be blocklisted, and resulted in **less crawler traffic**

	Successfully Crawled	Blocked Anywhere	Mean Time to Blocklisting	Mean Requests per Site
 w/ cloaking	61.4%	23.0%	238 min	162
No cloaking	97.4%	49.4%	126 min	334

- Key assumption: experimental design representative of ecosystem
- Abuse reports far slower



Cloaking Effectiveness



- **Mobile-only** sites never blocked anywhere
- + **no blacklist warnings** on mobile devices



- **US-only** sites never blocked by GSB
- **Non-US** sites never blocked by APWG & others



- **.htaccess** cloaking effective for first 12 hours

JavaScript



- **JavaScript** cloaking slowed blocking in long term

PhishFarm

- Framework Available: <https://phishfarm-project.com>
- Transitioning Framework to APWG
 - <https://ecrimeresearch.org/phishfarm/>
- Cloaking prolongs phishers' **window of opportunity**
 - Novel techniques to be expected
 - Geo-specific cloaking remains effective
- Mitigations **not fast enough** to prevent abuse
 - Blocklists
 - Hosting infrastructure
- Ecosystem must improve to keep users safe



Key Observation

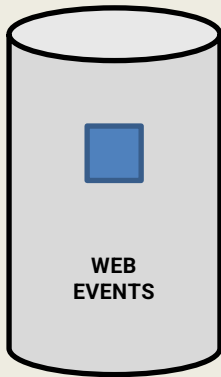
- Phishing kits “often” embed first-party JavaScript tracking code or images












Status	Method	Domain	File	Cause	Type	Transferred	Size	0 ms		
200	GET	ty364tsdsaf.appspot.com	8cc47449c8e0cc4c4f254cd03568bae9nabr1570557671.css	stylesheet	css	843 B	1.06 KB	1686 ms		
200	GET	ty364tsdsaf.appspot.com	b1821919c7bcc1049302e1f2e606f003nabr1570557671.css	stylesheet	css	24.05 KB	127 KB	1957 ms		
200	GET	ty364tsdsaf.appspot.com	37_533e293f0c8947ada653b47c00e394e2.png	img	png	1.99 KB	1.71 KB	1669 ms		
200	GET	ty364tsdsaf.appspot.com	microsoft_logo.svg	img	svg	1.84 KB	3.57 KB	1738 ms		
200	GET	ty364tsdsaf.appspot.com	ellipsis_white.svg	img	svg	605 B	915 B	1736 ms		
200	GET	ty364tsdsaf.appspot.com	ellipsis_grey.svg	img	svg	605 B	915 B	1737 ms		
200	GET	aadcdn.msftauth.net	0-small_138bcee624fa04ef9b75e86211a9fe0d.jpg	img	jpeg	3.54 KB	2.94 KB	41 ms		
200	GET	aadcdn.msftauth.net	0_a5dbd4393ff6a725c7e62b61df7e72f0.jpg	img	jpeg	277.41 KB	276.71 KB	68 ms		
200	GET	secure.aadcdn.microsofto...	favicon_a.ico	img	x-icon	17.10 KB	16.77 KB	84 ms		

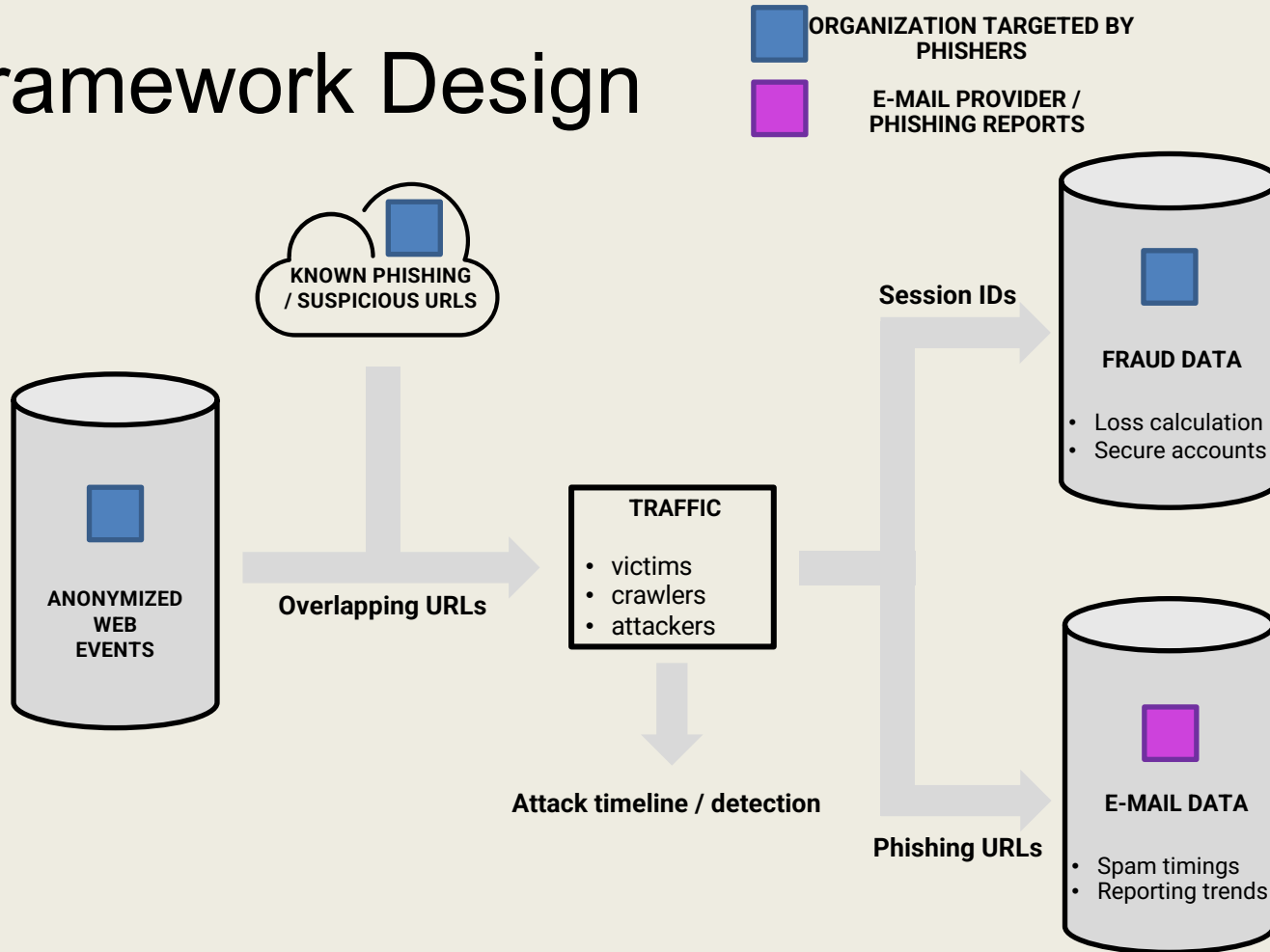
Building an Analysis Framework

 ORGANIZATION TARGETED BY PHISHERS





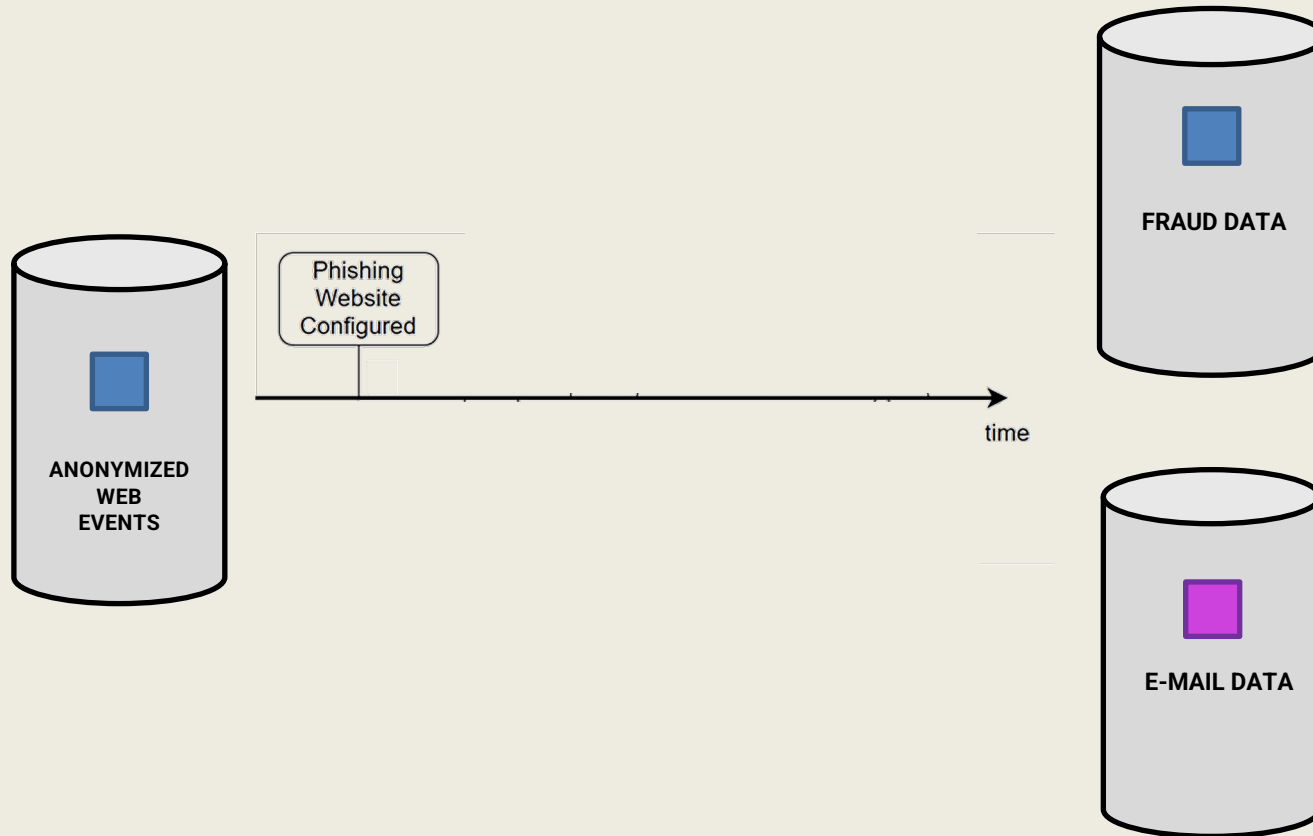
Status	Method	Domain	File	Cause	Type	Transferred	Size	0
200	GET	 ty364tsdsaf.appspot.com	8cc47449c8e0cc4c4f254cd03568bae9nbr1570557671.css	stylesheet	css	843 B	1.06 KB	
200	GET	 ty364tsdsaf.appspot.com	b1821919c7bcc1049302e1f2e606f003nbr1570557671.css	stylesheet	css	24.05 KB	127 KB	
200	GET	 ty364tsdsaf.appspot.com	37_533e293f0c8947ada653b47c00e394e2.png	img	png	1.99 KB	1.71 KB	
200	GET	 ty364tsdsaf.appspot.com	microsoft_logo.svg	img	svg	1.84 KB	3.57 KB	
200	GET	 ty364tsdsaf.appspot.com	ellipsis_white.svg	img	svg	605 B	915 B	
200	GET	 ty364tsdsaf.appspot.com	ellipsis_grey.svg	img	svg	605 B	915 B	
200	GET	 aadcdn.msftauth.net	0-small_138bcee624fa04ef9b75e86211a9fe0d.jpg	img	jpeg	3.54 KB	2.94 KB	
200	GET	 aadcdn.msftauth.net	0_a5dbd4393ff6a725c7e62b61df7e72f0.jpg	img	jpeg	277.41 KB	276.71 KB	
200	GET	 secure.aadcdn.microsofto...	favicon_a.ico	img	x-icon	17.10 KB	16.77 KB	

Framework Design





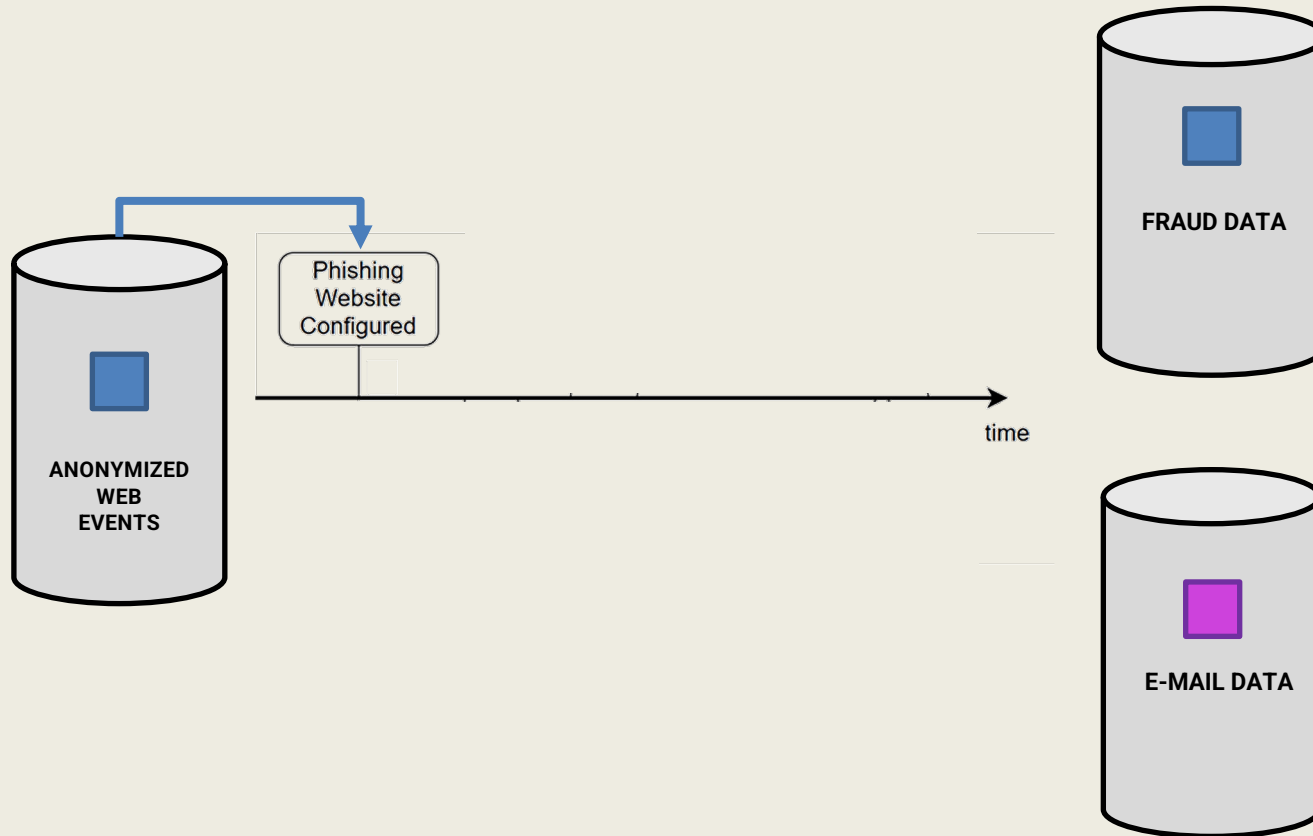
End-to-end Timeline

-  ORGANIZATION TARGETED BY PHISHERS
-  E-MAIL PROVIDER / PHISHING REPORTS





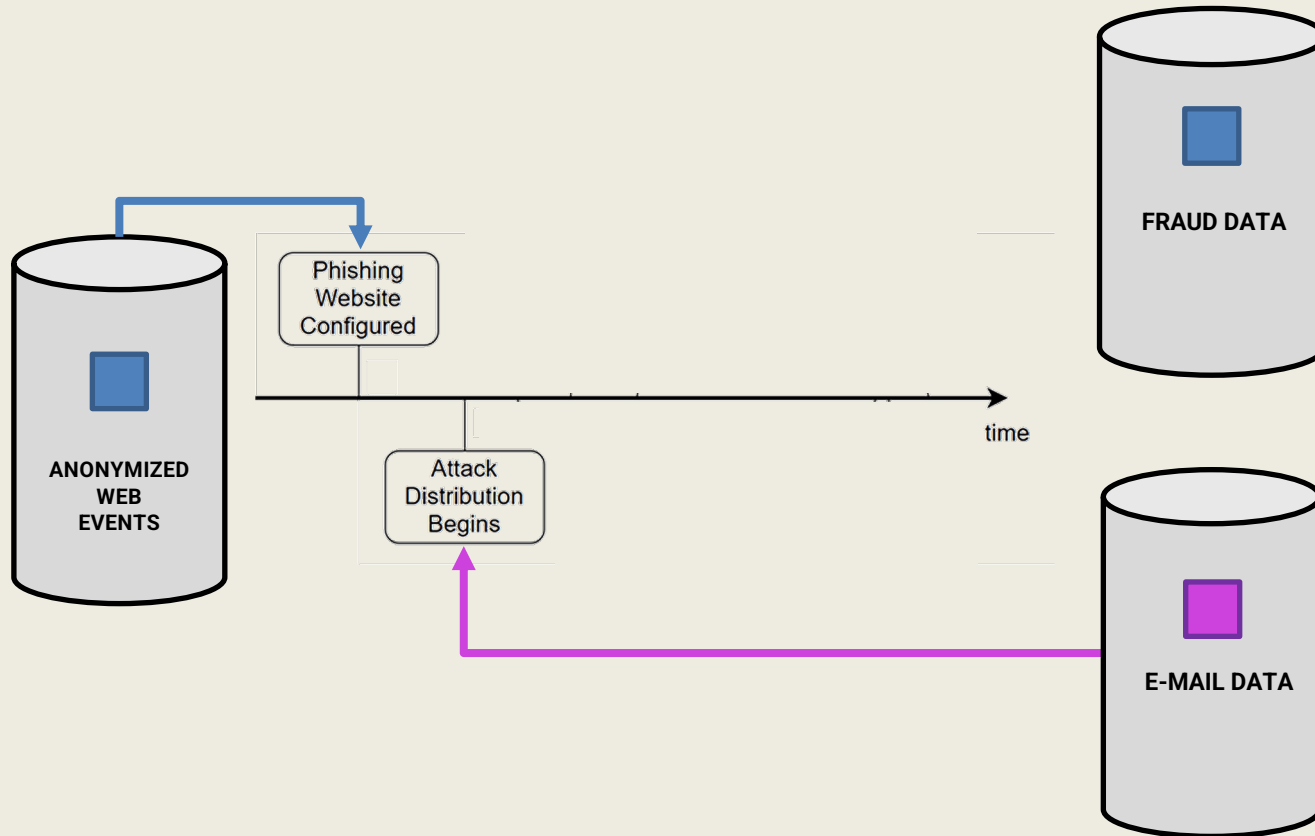
End-to-end Timeline

-  ORGANIZATION TARGETED BY PHISHERS
-  E-MAIL PROVIDER / PHISHING REPORTS

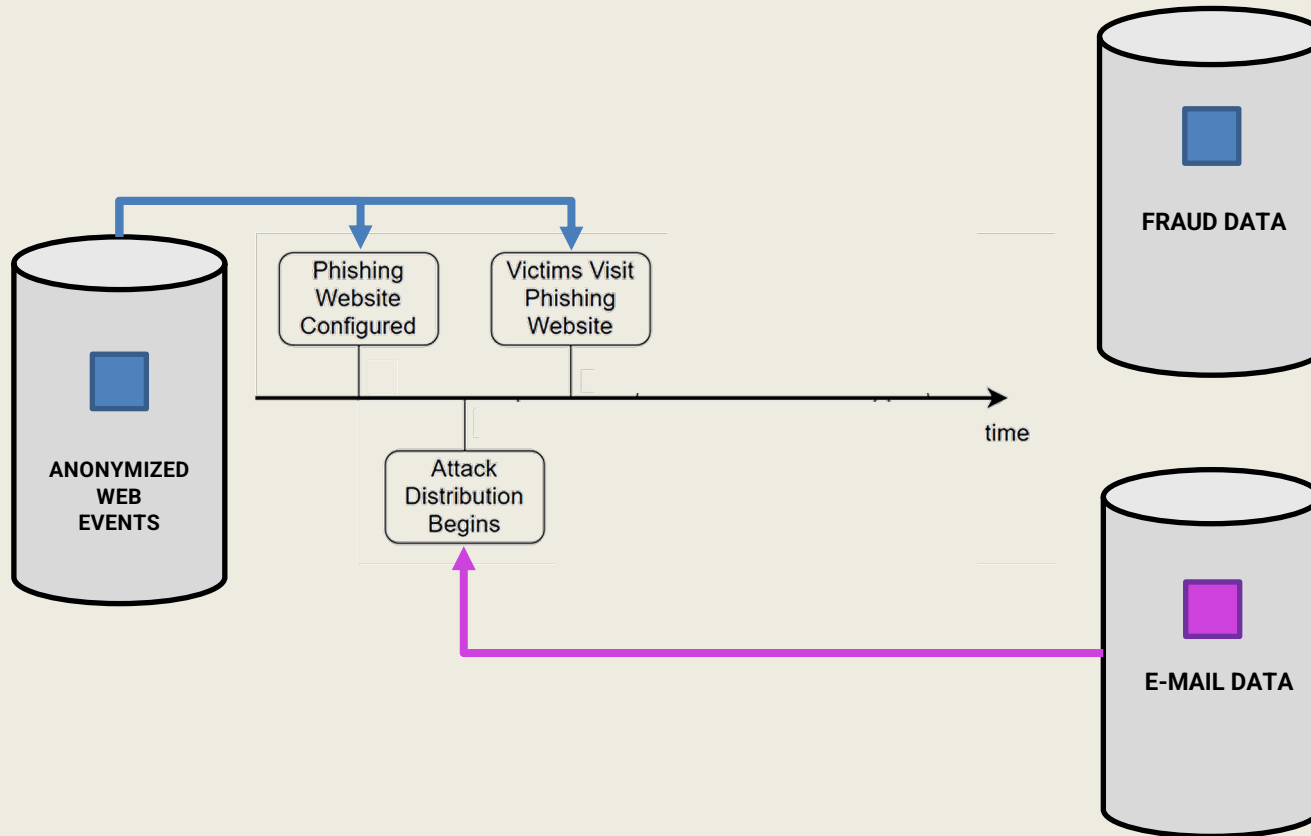
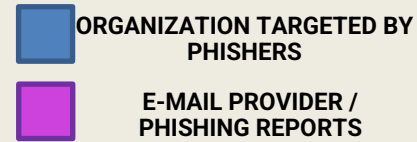


End-to-end Timeline

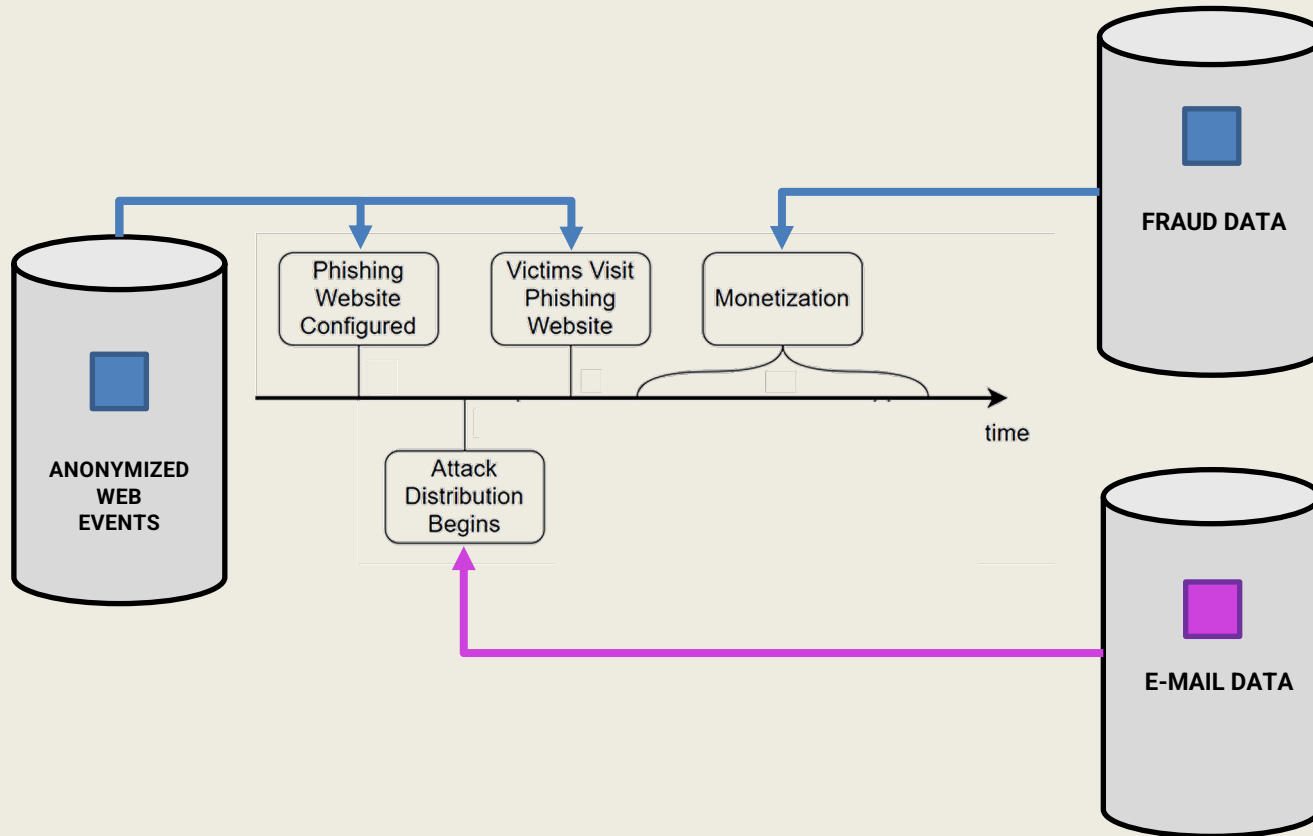
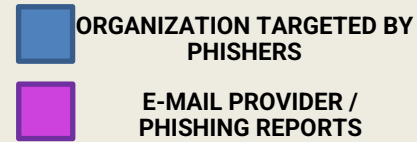
-  ORGANIZATION TARGETED BY PHISHERS
-  E-MAIL PROVIDER / PHISHING REPORTS



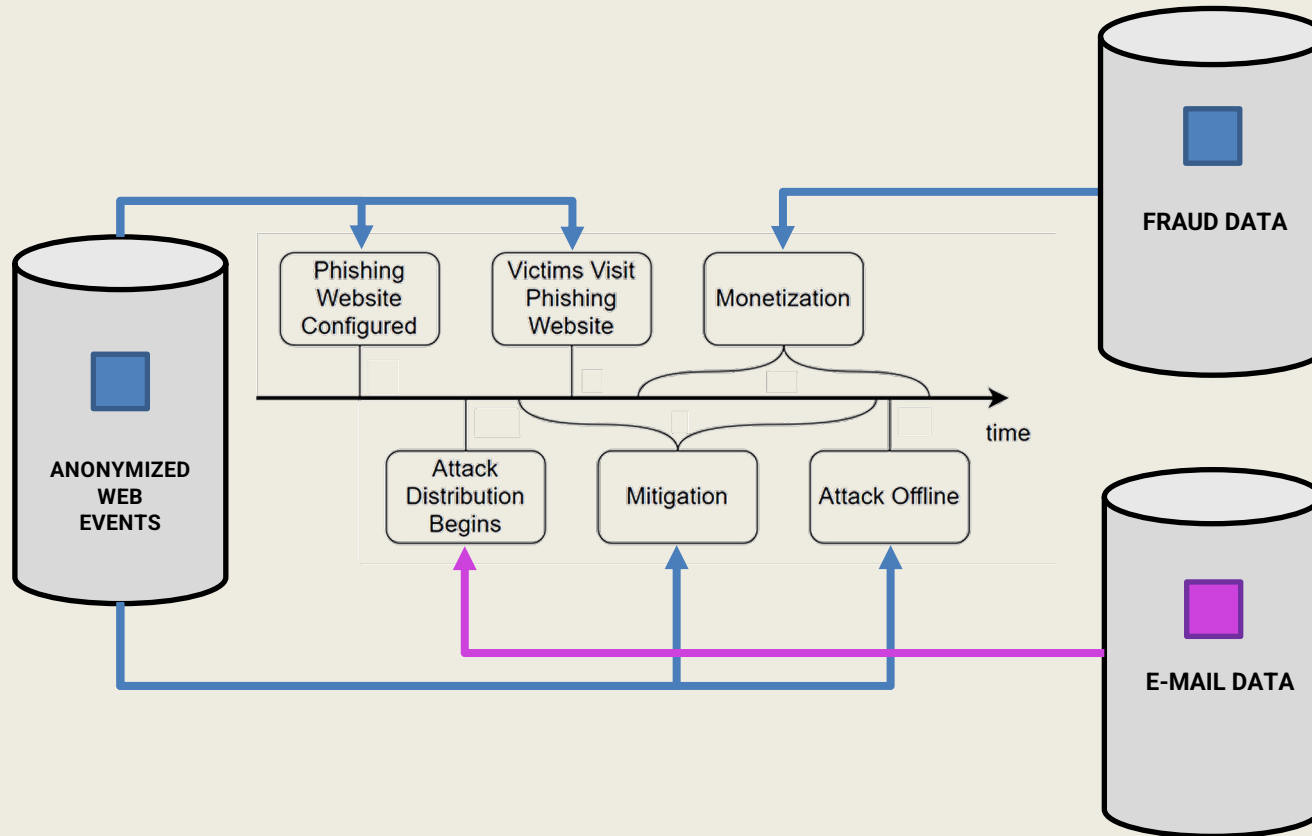
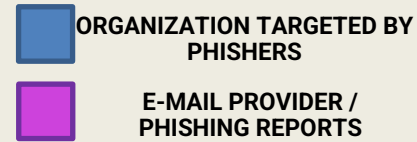
End-to-end Timeline



End-to-end Timeline



End-to-end Timeline



“Golden Hour” Data Set

- **Source:** large organization (top 10 most-phished)



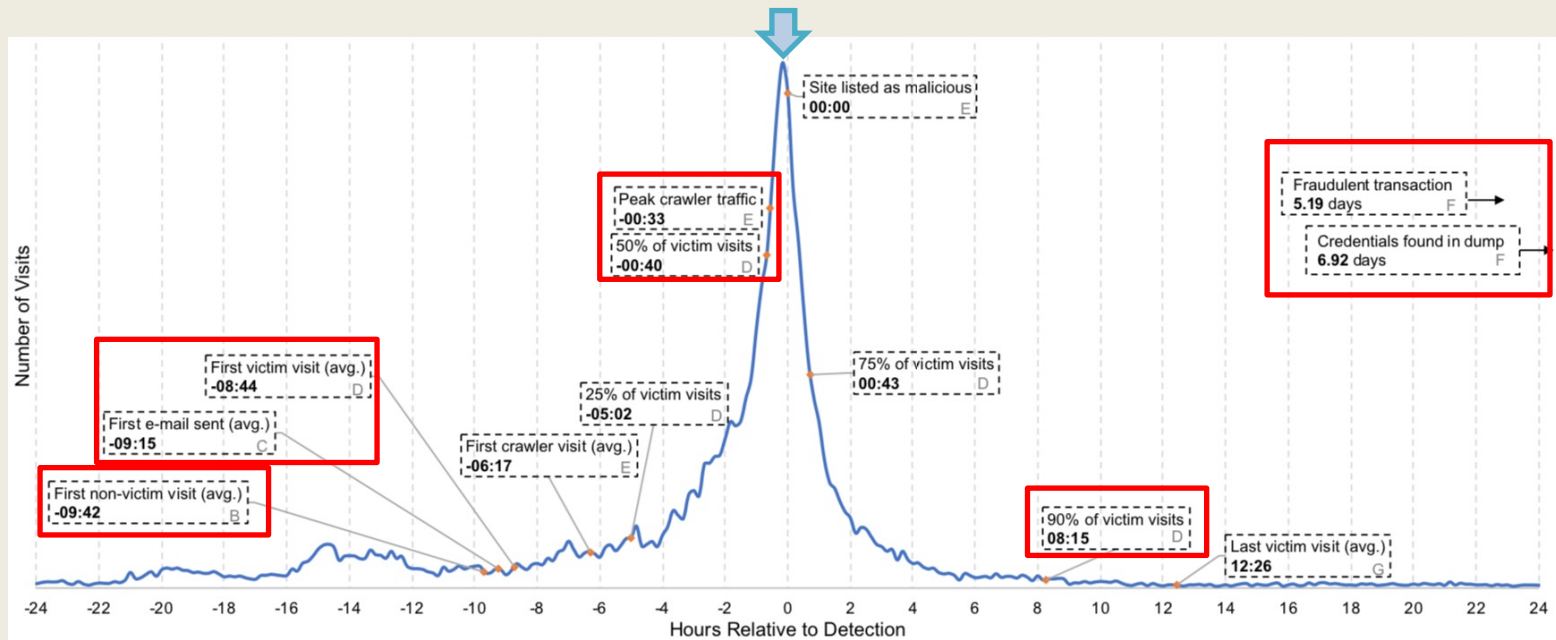
- **Visibility:** 39.1% of known phishing domains

	Trackable by Golden Hour		Estimated Total
	Potential Victims	Known User	
Phishing Site Page Loads	15.6M	4.8M	39.9M
Suspected Successful Phish	482K	148K	1.2M

7.6% phishing success rate



End-to-end Timeline of Phishing



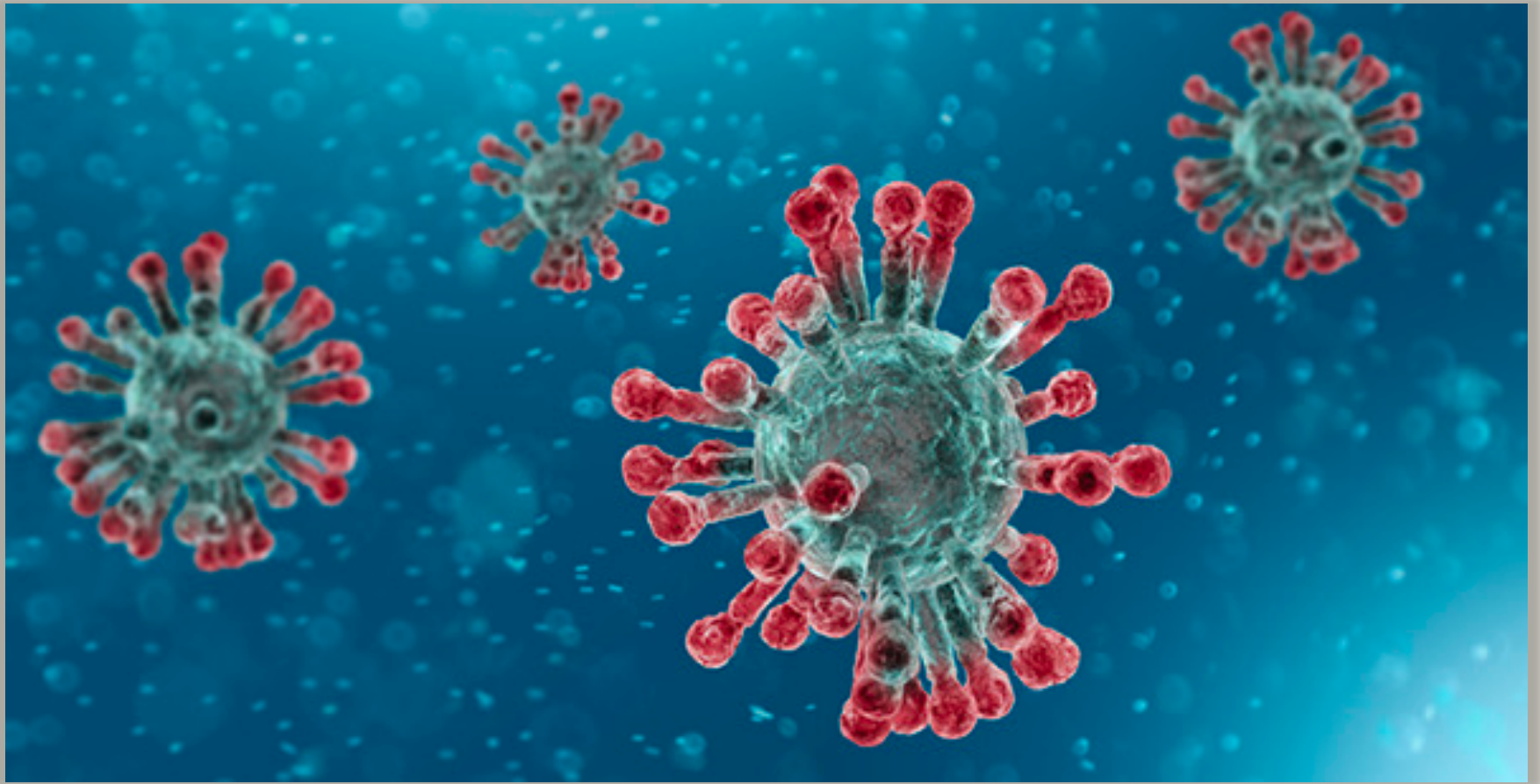
Proactive
detection

Reactive mitigation improvements

Secure affected user accounts



Coronavirus



Motivation

Отвечить Ответить всем Переслать

От Corona Support <info@██████████.com> ☆

Тема CDC HEALTH emergency coronavirus (2019-nCoV) News

Обратный адрес info@██████████.com ☆

Кому tom0184@██████████.tw ☆

Dear Sir/Madam

The center for disease control and Prevention (CDC) continues to work to go all out to control an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China, that began in December 2019. Updated list of new case around your city are available at (www.cdc.gov/coronavirus/2019).

CDC has established an incident management system for domestic and international public health emergency response. Funding of the above project is dependent on your good will donation, nothing is guaranteed amount.

This e-plate form for your contribution to our public health emergency response. If you are interested, please contact us together, we will be happy to help you. All information is confidential and working round the clock to find a way to help you.

Please kindly find our Bitcoin account to support.

17iiciHtCDF0mEpdmhJ43DtnkGvWgjiXVm

Thanks you for your goodwill contribution to our public health emergency response. You are a hero. Please help us as much as possible.

Sincerely

CDC-INFO National Contact Center for domestic and international public health emergency response
National Center for Health Marketing
<https://www.cdc.gov/coronavirus/index.html>
Division of eHealth Marketing
Center for Disease Control and Prevention
info@cdc.gov

COMPONENTS direct Order Online or Call 01623 788 400 Log in Register Request a Catalogue


Industrial Fasteners Industrial Hardware Furniture Hardware Furniture Assembly Components More

Search here... YOUR BASKET £0.00

Home / More / safety / Face Shield Visors

Face Shield Visors

Details Prices



These disposable Face Shield Visors are clear and cover the whole face to protect the wearer from droplets and liquid splashes and will provide protection against Covid-19. They are fitted with an elasticated strap for a comfortable fit. Ideal for key workers, hairdressers, construction workers, shop and office workers, beauty salons etc.

Protects eyes, nose and mouth against splashes, dust and aerosols
Prevents the wearer from touching face and spreading contamination
Reduces the risk of cross contamination
Does not contain any natural rubber
Anti-fog coating prevents mist obscuring vision
Clear optics, minimal distortion to vision, and does not obstruct facial expressions
Shatter proof
Does not obstruct the airways, and allows normal breathing and does not restrict communication
Single size fits all
Facial expressions and smiles remain visible
Made in the UK from over 85 percent locally sourced materials

Putting on the Face Shield
1. Wash your hands with soap and water (or hand sanitiser) before touching the Face Shield.
2. Reach up to your forehead and use the clear plastic to rest against your forehead.
3. Press the elastic strap over the crown of your head.
4. Adjust the strap to fit your head and face and ensure it is comfortable.
5. Press the strap against your forehead to ensure the visor is secure.

Removing the Face Shield
1. Wash your hands with soap and water (or hand sanitiser) before touching the Face Shield.
2. Reach back to touch the elastic strap.
3. Do not touch the front of your Face Shield as it may be contaminated.
4. Lift the elastic up and over your head and remove the Face Shield from your face.
5. Discard the Face Shield.
6. Clean your hands again using soap and water or hand sanitiser

Important Safety Information
This PPE is designed for Single Use only, by one user. It must not be shared. We do not recommend multiple session use. COVID-19 can remain on hard surfaces for up to 3

SAVE FOR REFERENCE ASK A QUESTION ABOUT THIS ITEM

and much more ...

User name:

Password:

sign in



Approach

- We collected a comprehensive dataset and analyzed it to identify the trends:



News articles and announcements



Victim visits on phishing websites



DNS records and TLS certificates



Reported phishing emails



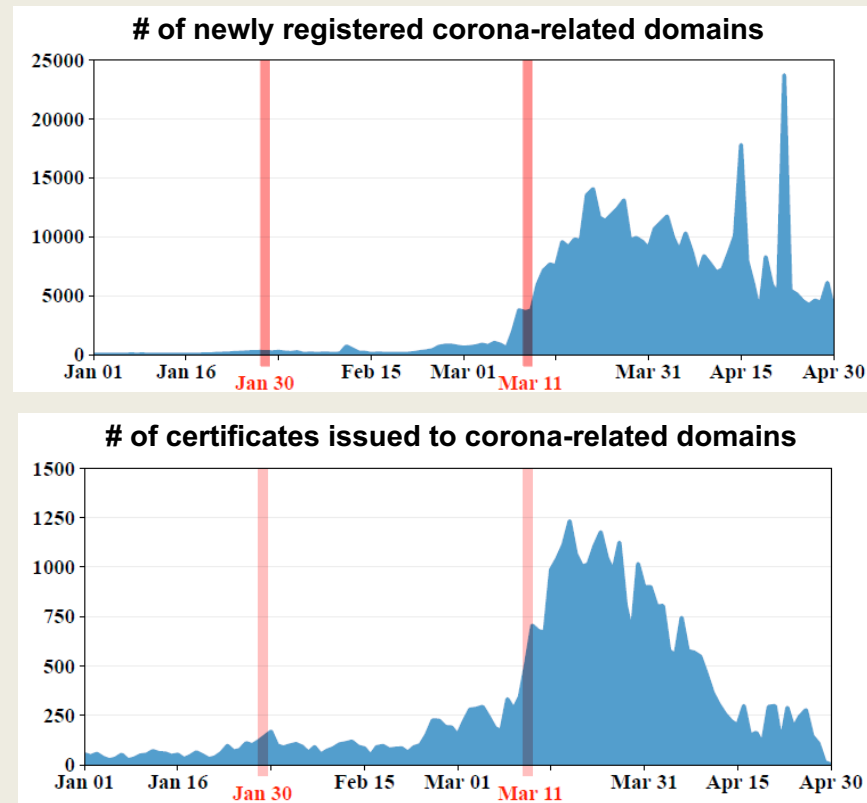
Source code of malicious websites



Underground forum discussions

Domain Names and TLS Certificates

The number of corona-related domain names started increasing from early March 2020 after W.H.O. declared a pandemic



The W.H.O. declared a global health emergency

The W.H.O. declared the outbreak of COVID-19 a pandemic



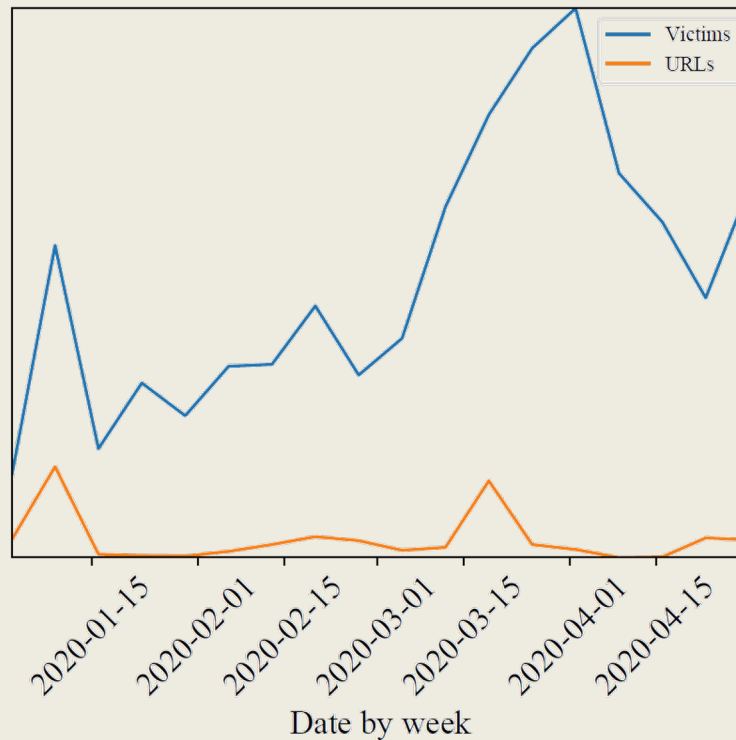
Phishing Trends

- The number of phishing hostnames reported to two major clearinghouses did not increase
- We analyzed phishing emails and traffic to phishing websites at one major industry organization using GoldenHour framework

Phishing Trends

Through an increase in spamming activity against a larger attack surface, the pandemic led to record numbers of phishing victims

Victim visits to phishing websites

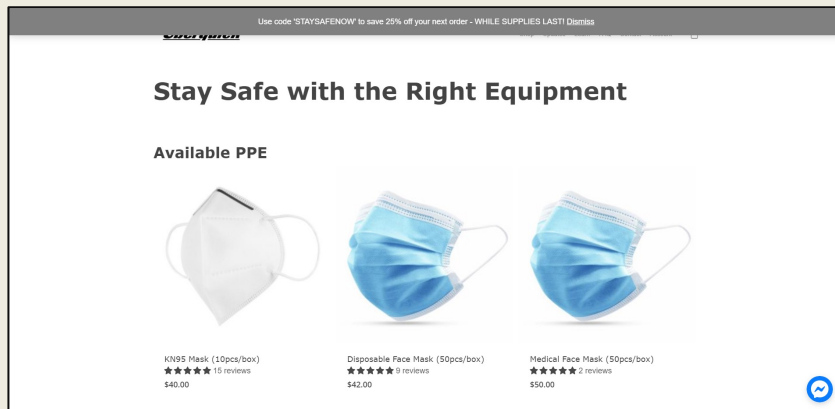
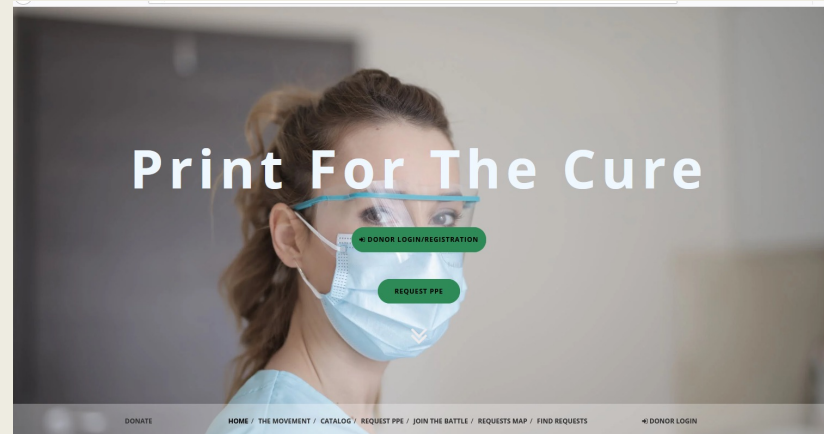


COVID-19 Themed Phishing

We crawled the source of 49K scam and phishing websites

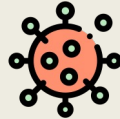


Donation-themed



PPE Sale

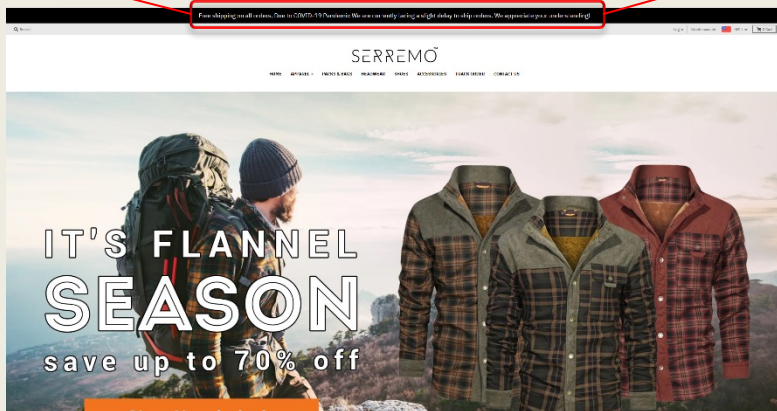
COVID-19 Themed Phishing



Corona-related Events

A screenshot of a phishing form titled "COVID-19 Pandemic Scenarios & Benefits Available" with the IRS logo in the top right. The form asks for "Enter the following information to update your COVID-19 Income Benefit Return Information." and lists "Required fields" including: Social Security Number (or Individual Taxpayer Identification Number), First Name, Last Name, Address (Number and Street), Date of Birth (MM/DD/YYYY), Direct Deposit (Select One), Bank Name, Account Number, Routing Number, Bank Address, Country (United States), City/County/Province, State/U.S. Territory (Select One), and ZIP Code/Postal Code. A "Submit" button is at the bottom right, and a link for "IRS Privacy Policy | Privacy Notice" is at the bottom left.

Free shipping on all orders. Due to COVID-19 Pandemic We are currently facing a slight delay to ship orders. We appreciate your understanding!



Shopping Websites



Key Takeaways

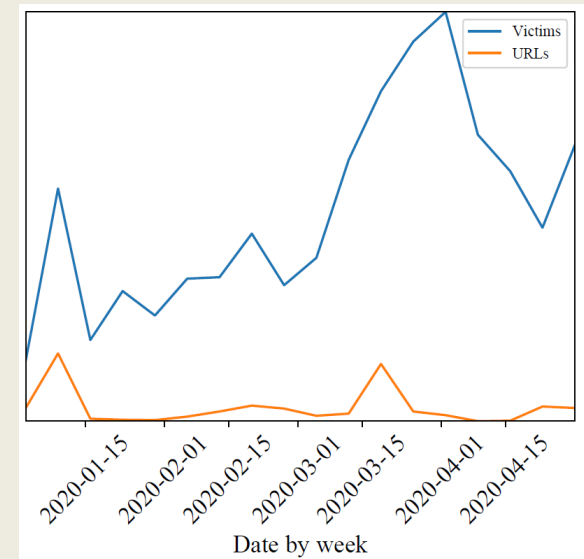
- Attackers favor general phishing websites while taking advantage of the pandemic in other contexts
- Reactive anti-phishing systems are not enough

The number of corona-related URLs reported to the APWG

Month	# of Reported URLs	# of HTTPS Domains
Jan 2020	0	0
Feb 2020	5	1
Mar 2020	171	37
Apr 2020	140	34
Total	316	72

~~467,323~~

Victims visits to phishing websites



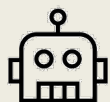
Key Takeaways (cont'd)

- 1 Low number of corona-related legitimate websites despite large number of registered domains
- 2 FTC report shows users lost \$40M to COVID-19 fraud from January to May*



Phishing is just one type of many corona-related attacks.
Cybercriminals use domains for different fraudulent purposes

Revisiting Cloaking

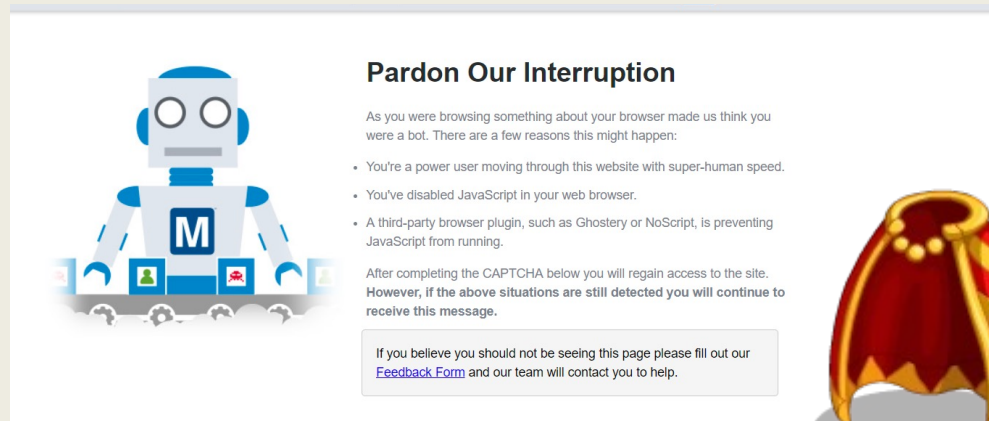


<https://verify-webscrid2367.serveirc.com/signin>



Cloaking

<https://verify-webscrid2367.serveirc.com/signin>

A screenshot of a web page with a white background. On the left is a blue robot with a white 'M' on its chest. To its right is the heading 'Pardon Our Interruption' followed by a paragraph of text and a bulleted list. Below the list is another paragraph and a feedback form box. On the right side of the screenshot is a red and yellow patterned hood.

Pardon Our Interruption

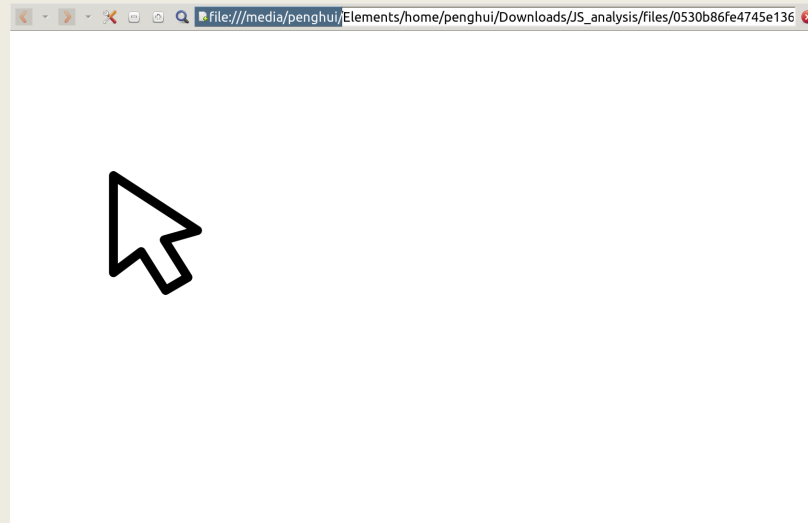
As you were browsing something about your browser made us think you were a bot. There are a few reasons this might happen:

- You're a power user moving through this website with super-human speed.
- You've disabled JavaScript in your web browser.
- A third-party browser plugin, such as Ghostery or NoScript, is preventing JavaScript from running.

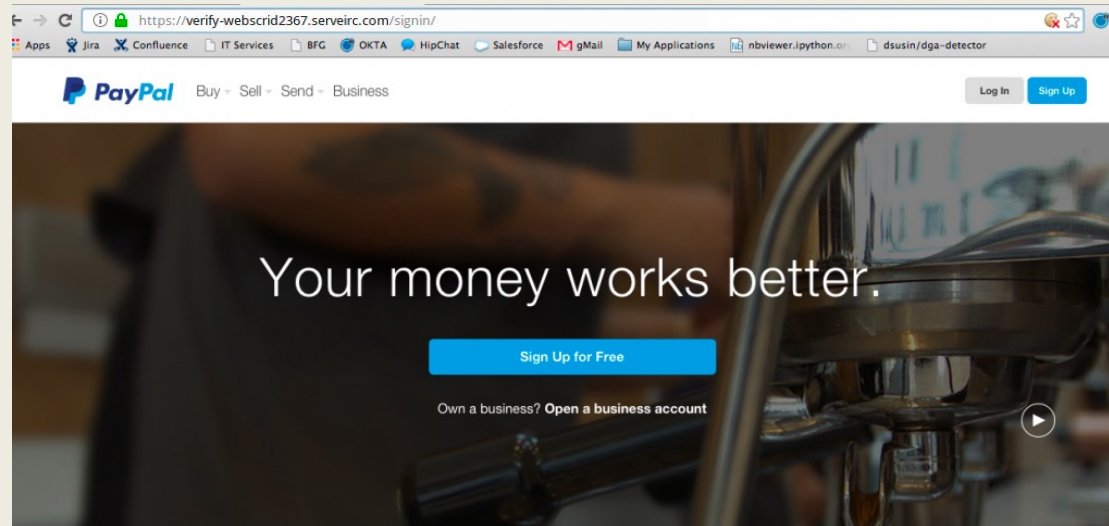
After completing the CAPTCHA below you will regain access to the site. However, if the above situations are still detected you will continue to receive this message.

If you believe you should not be seeing this page please fill out our [Feedback Form](#) and our team will contact you to help.

Cloaking



Cloaking



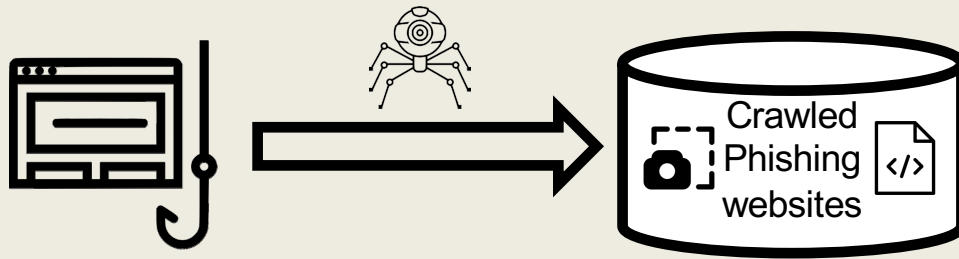
Architecture

Data Collection



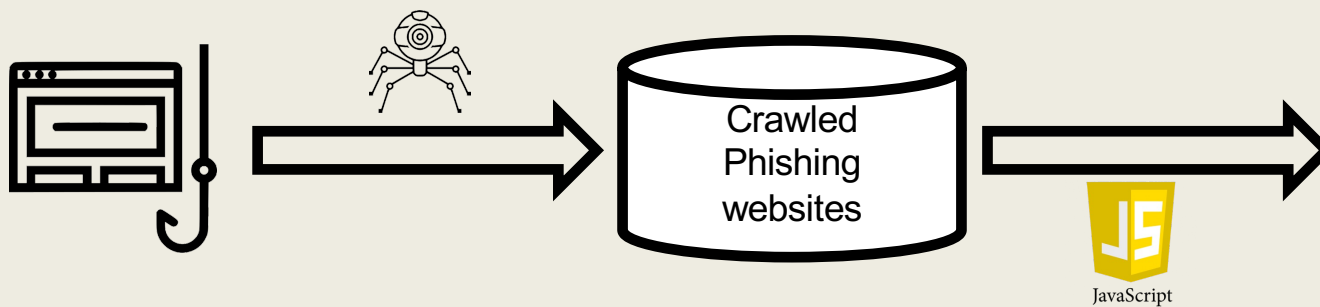
Architecture

Data Collection



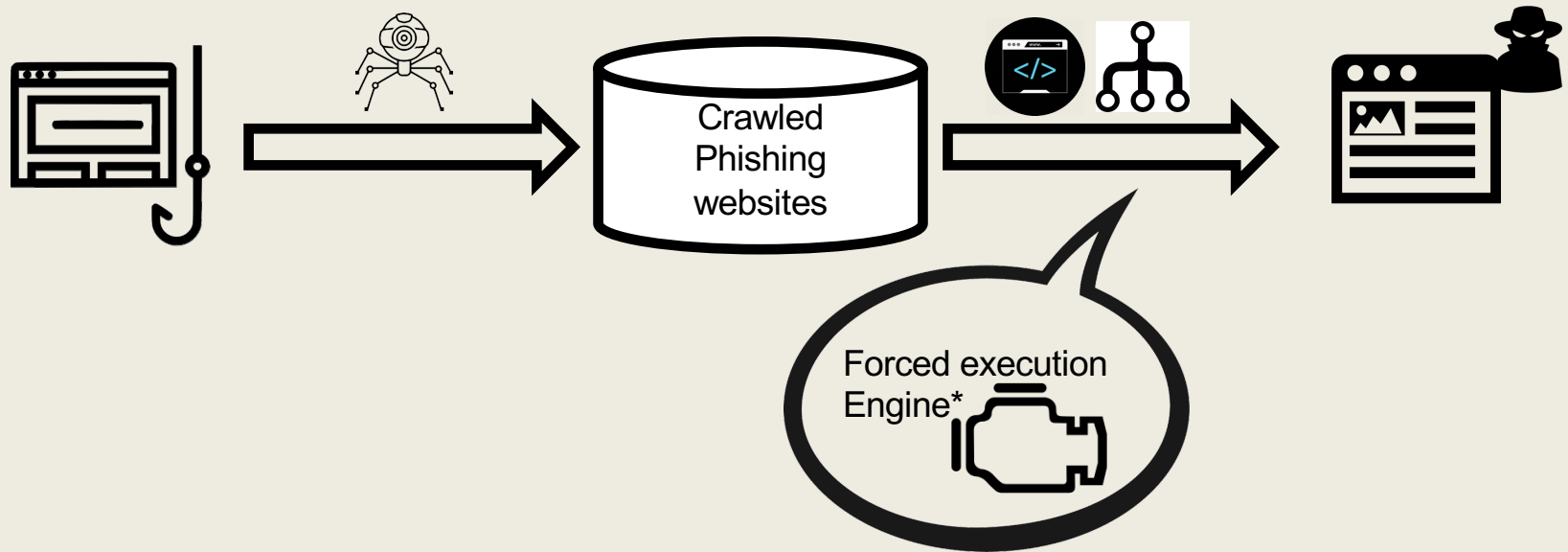
Architecture

Data Collection



Architecture

Data Collection

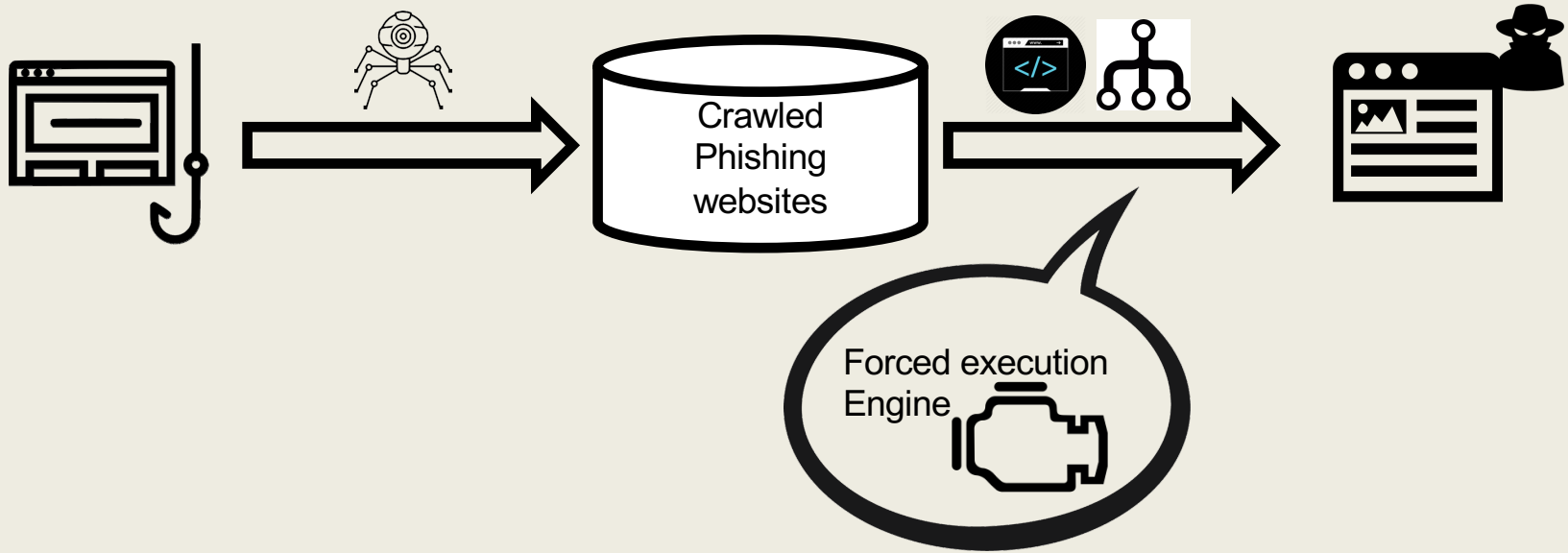


[*] J-Force: Forced Execution on JavaScript

Kyungtae Kim, I Luk Kim, Chung Hwan Kim, Yonghwi Kwon, Yunhui Zheng, Xiangyu Zhang, Dongyan Xu
26th international conference on World Wide Web, 2017

Architecture

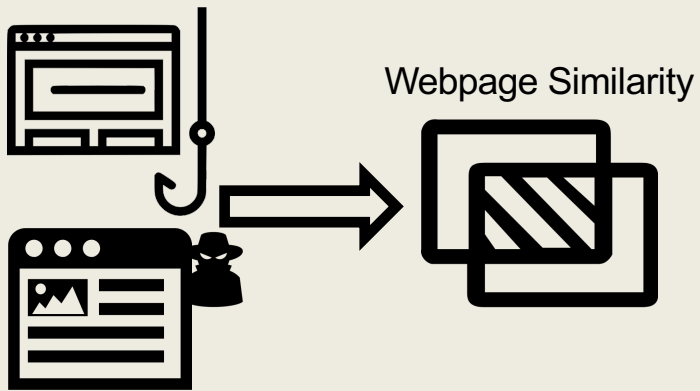
Data Collection



Analysis Engine

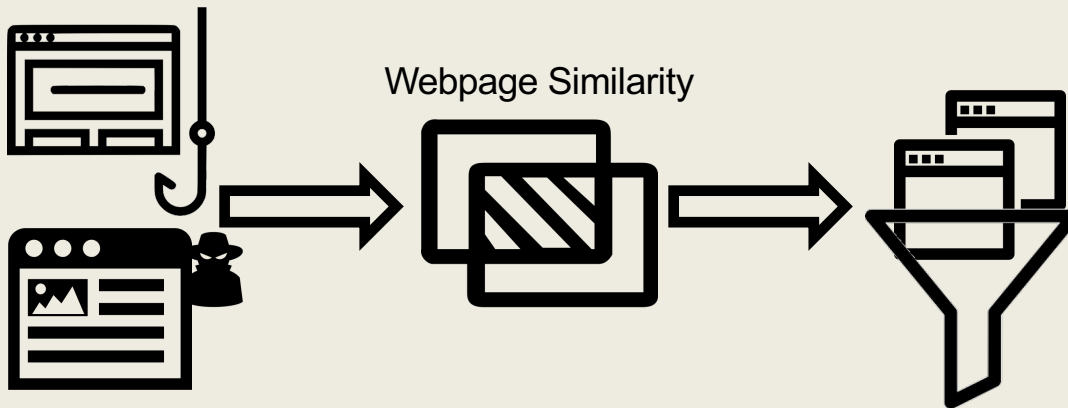
Architecture

Analysis Engine



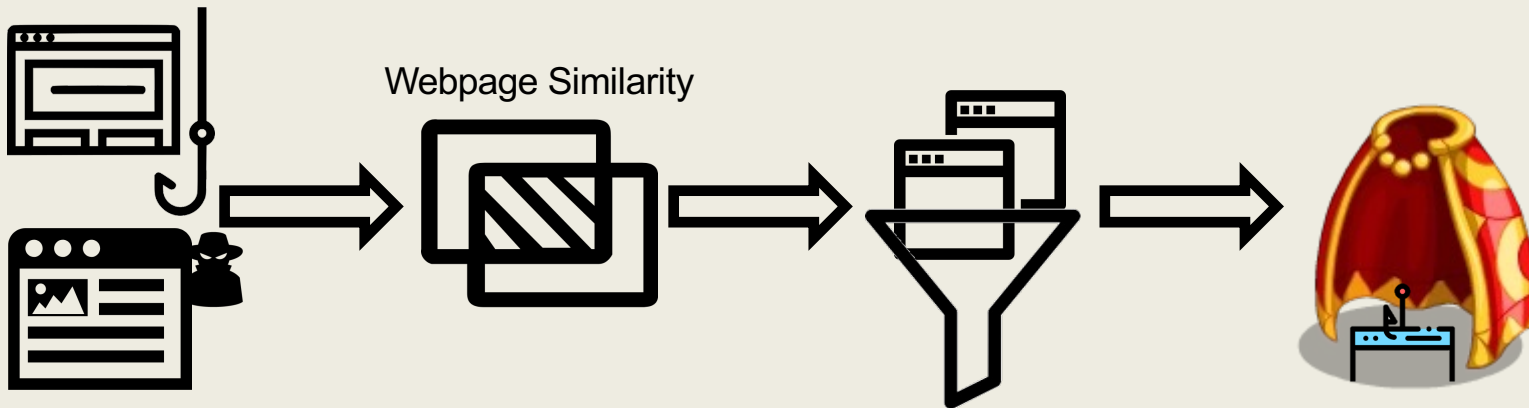
Architecture

Analysis Engine



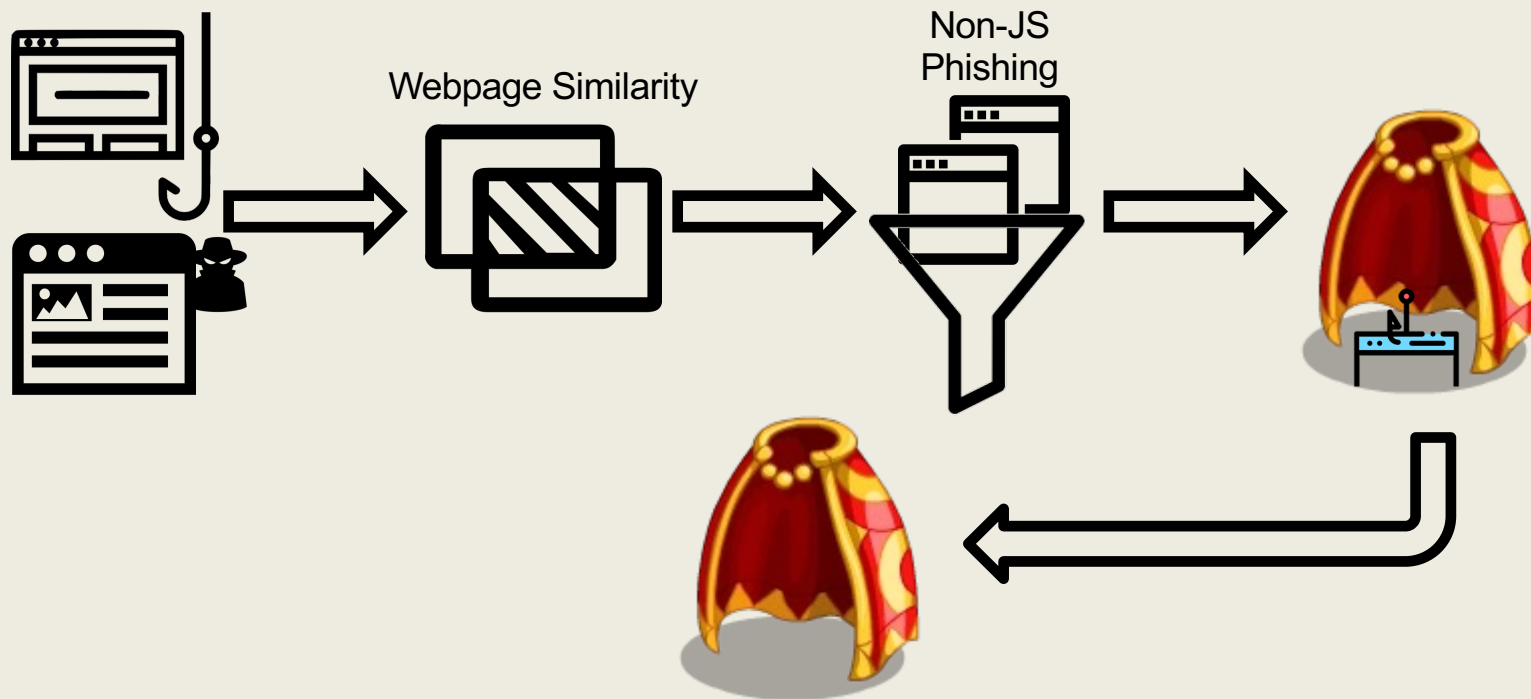
Architecture

Analysis Engine



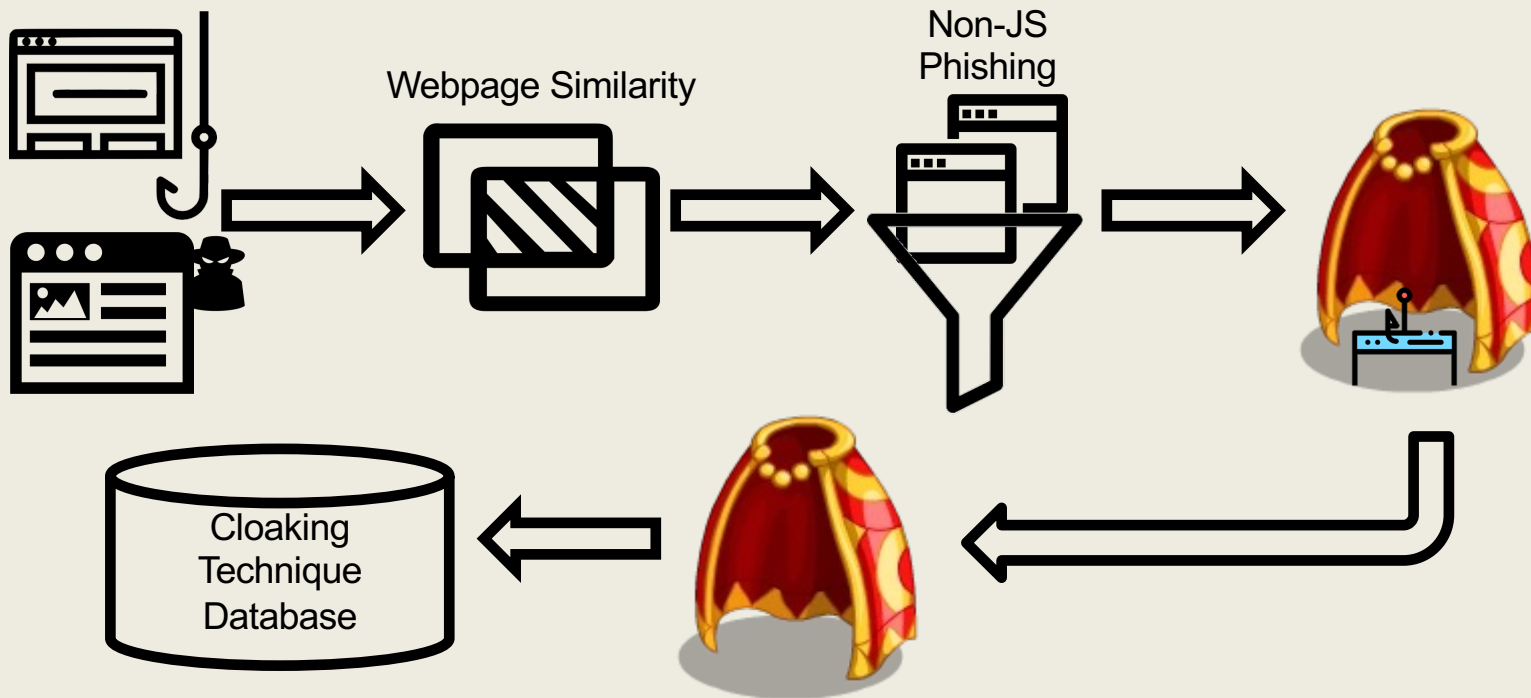
Architecture

Analysis Engine



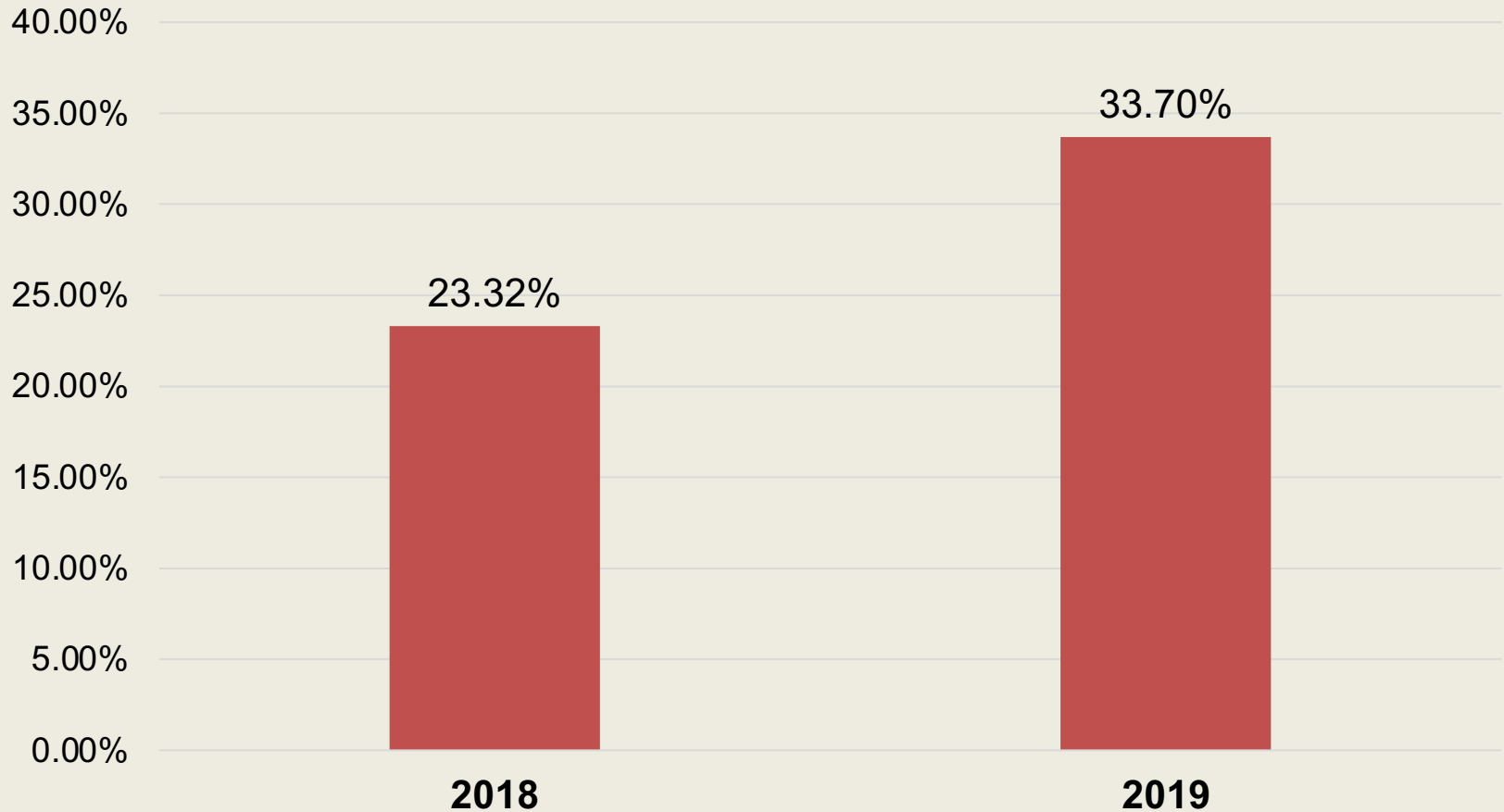
Architecture

Analysis Engine

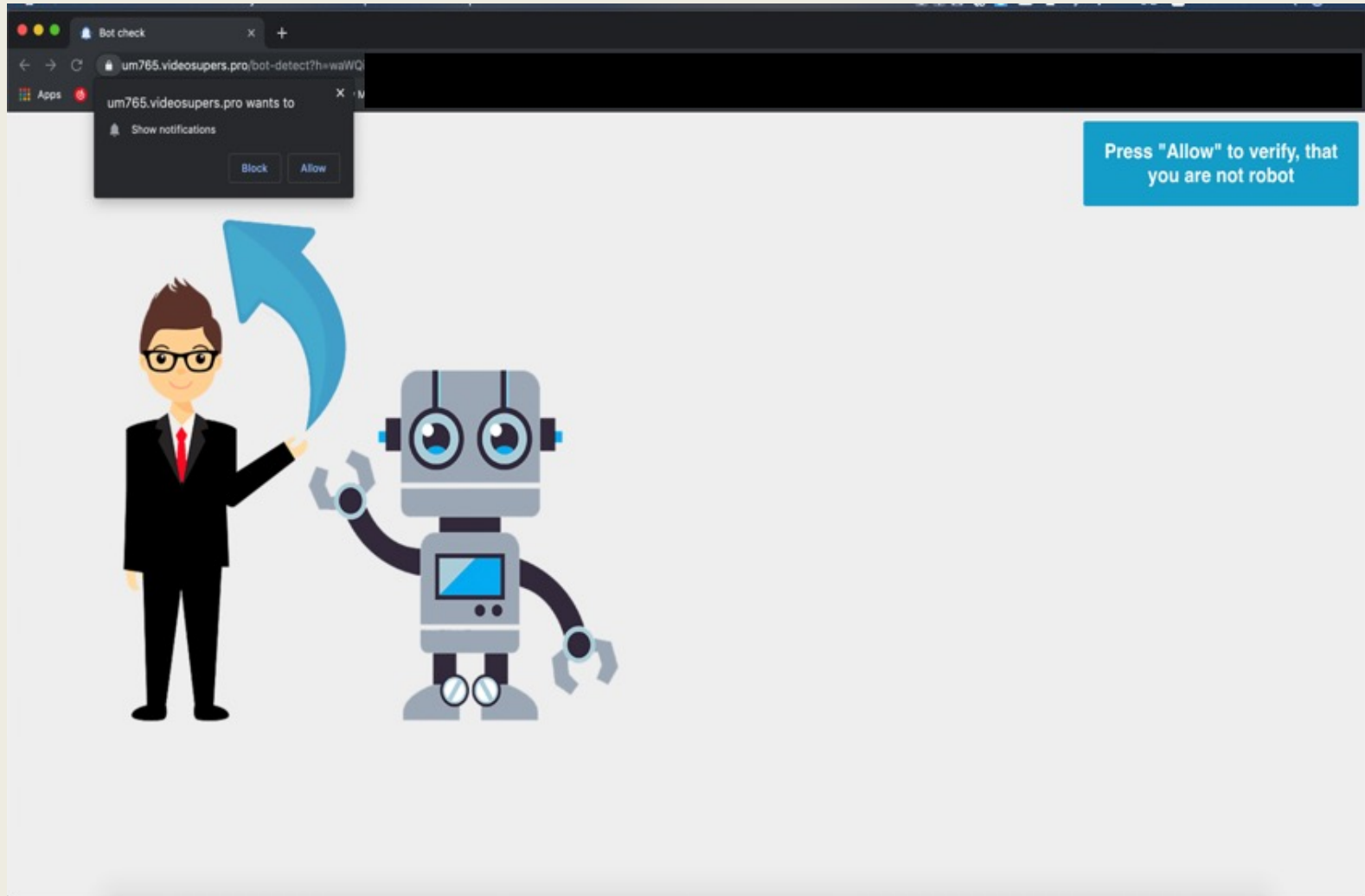


Cloaked Phishing Over Time

JS Cloaked Websites (%)



User Interaction



Impact

- Can these techniques truly evade detection by anti-phishing systems?
- Do they generally not discourage victim visits?

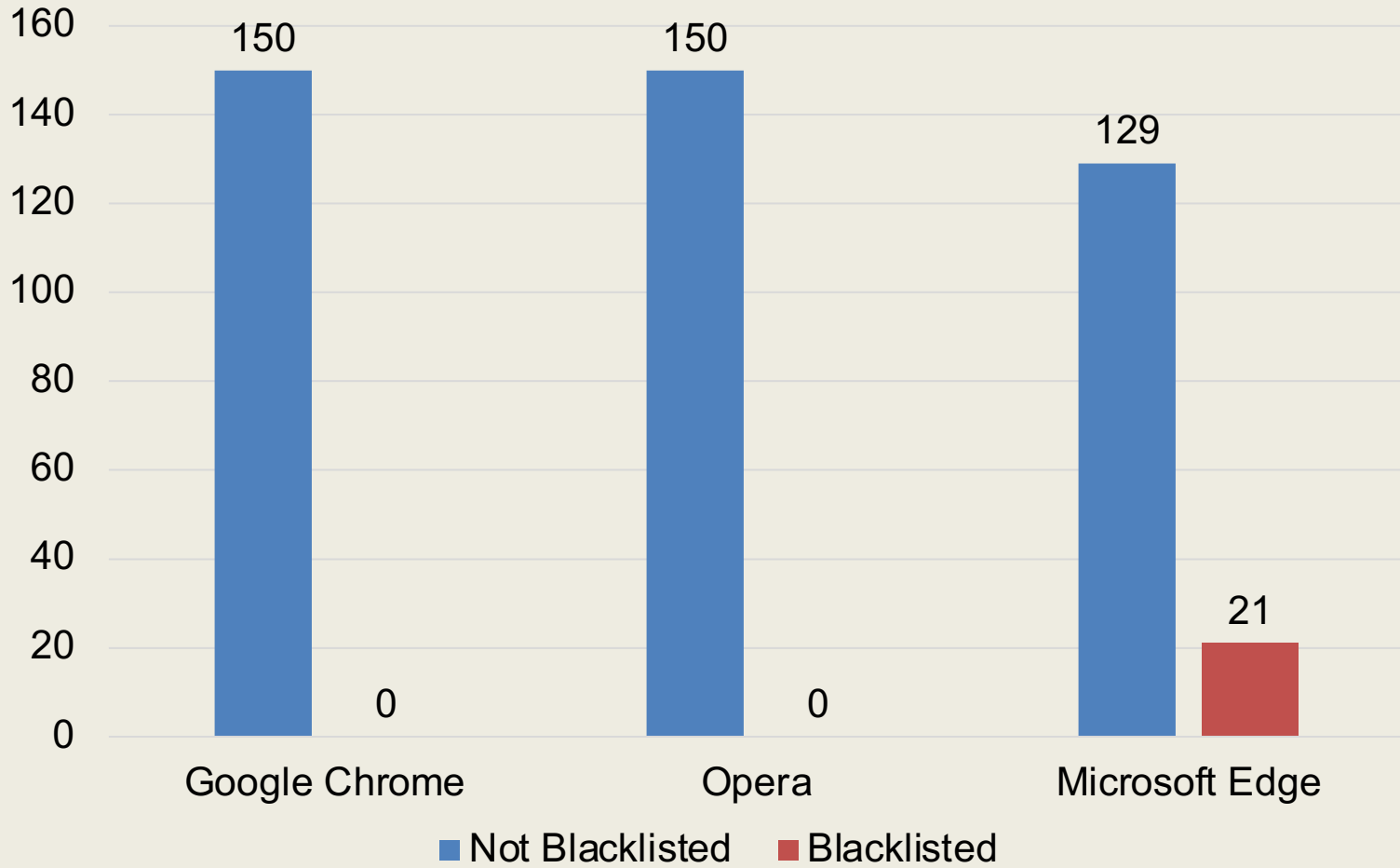


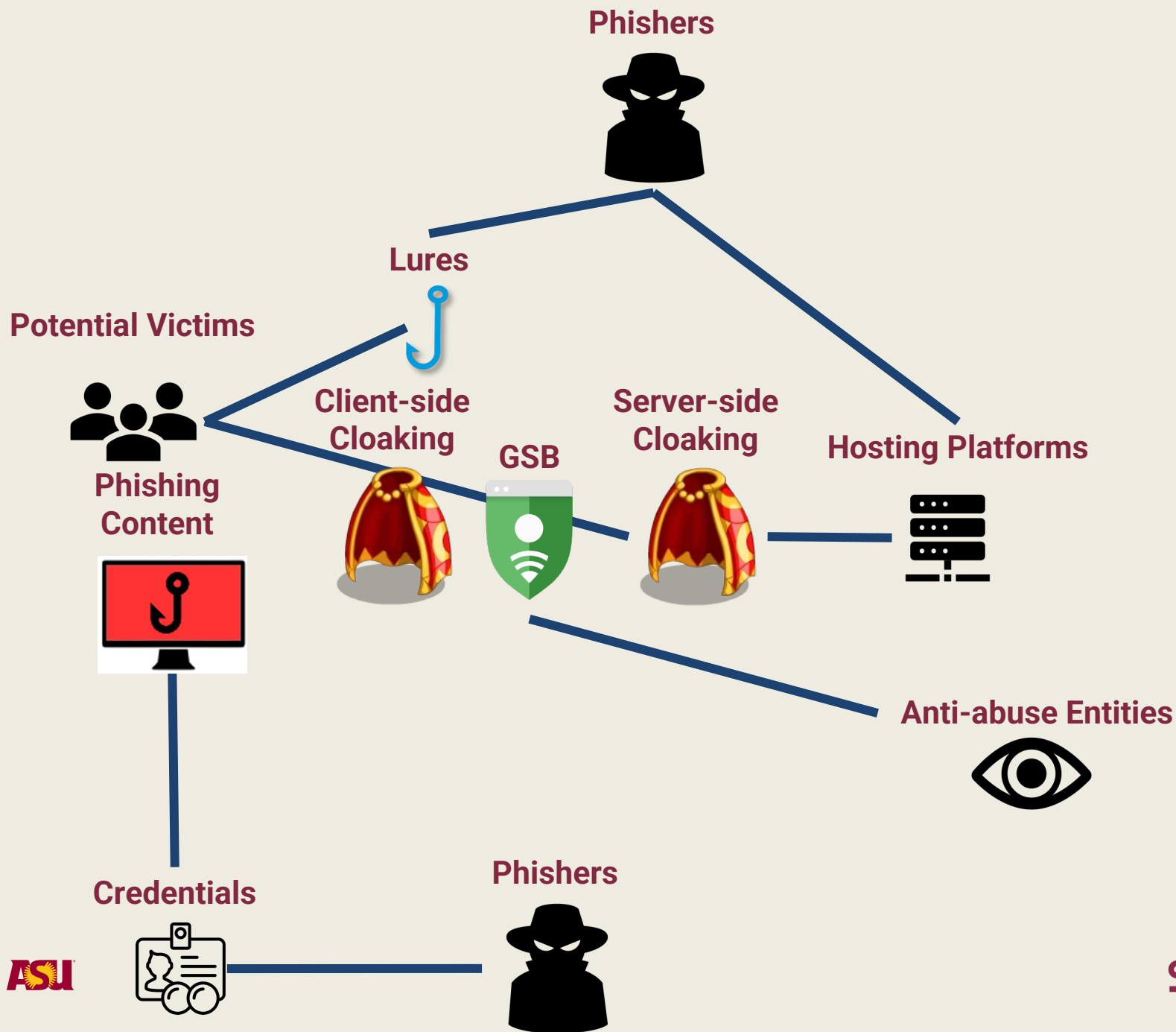
Effectiveness

User Interaction Cloaking



Results





Conclusions

- Extending beyond phishing
- Extending deeper into phishing
 - Advanced web phishing
 - Other phishing lures: SMS, voice, chat (whatsapp, etc.)
- Prevention
 - Removing incentives?
 - Education?

Adam Doupé

doupe@asu.edu

<https://sefcom.asu.edu>

WILD WILD PHISH: PHRONTIERS IN THE PHIGHT AGAINST PHISHING

