

# **Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale**

Adam Oest, Penghui Zhang, Adam Doupé, Gail-Joon Ahn  
Arizona State University

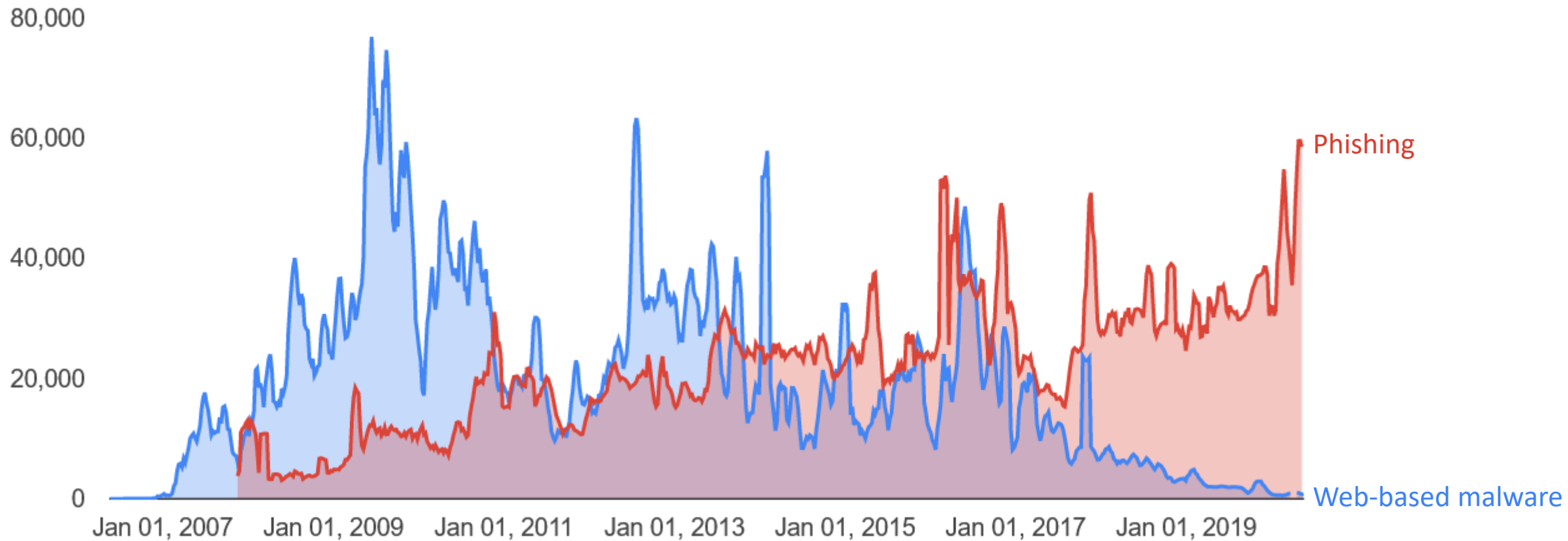
Brad Wardman, Eric Nunes, Jakub Burgis  
PayPal

Ali Zand, Kurt Thomas  
Google



# Phishing is Growing as Malware Declines

Weekly Malicious Website Detections <sup>[1]</sup>



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

# Outlook



## Sign in

to continue to Outlook

Email address, phone number, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

[Sign-in options](#)

Next

# Key Observation

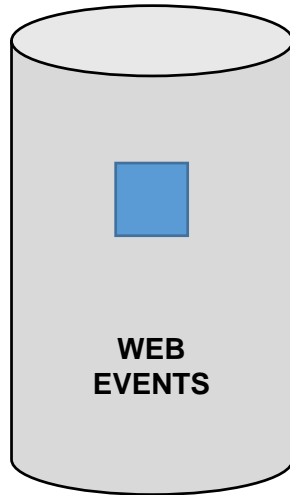
- Phishing kits “often” embed first-party JavaScript tracking code or images



Status	Method	Domain	File	Cause	Type	Transferred	Size	0 ms		
200	GET	ty364tsdsaf.appspot.com	8cc47449c8e0cc4c4f254cd03568bae9nbr1570557671.css	stylesheet	css	843 B	1.06 KB		1686 ms	
200	GET	ty364tsdsaf.appspot.com	b1821919c7bcc1049302e1f2e606f003nbr1570557671.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

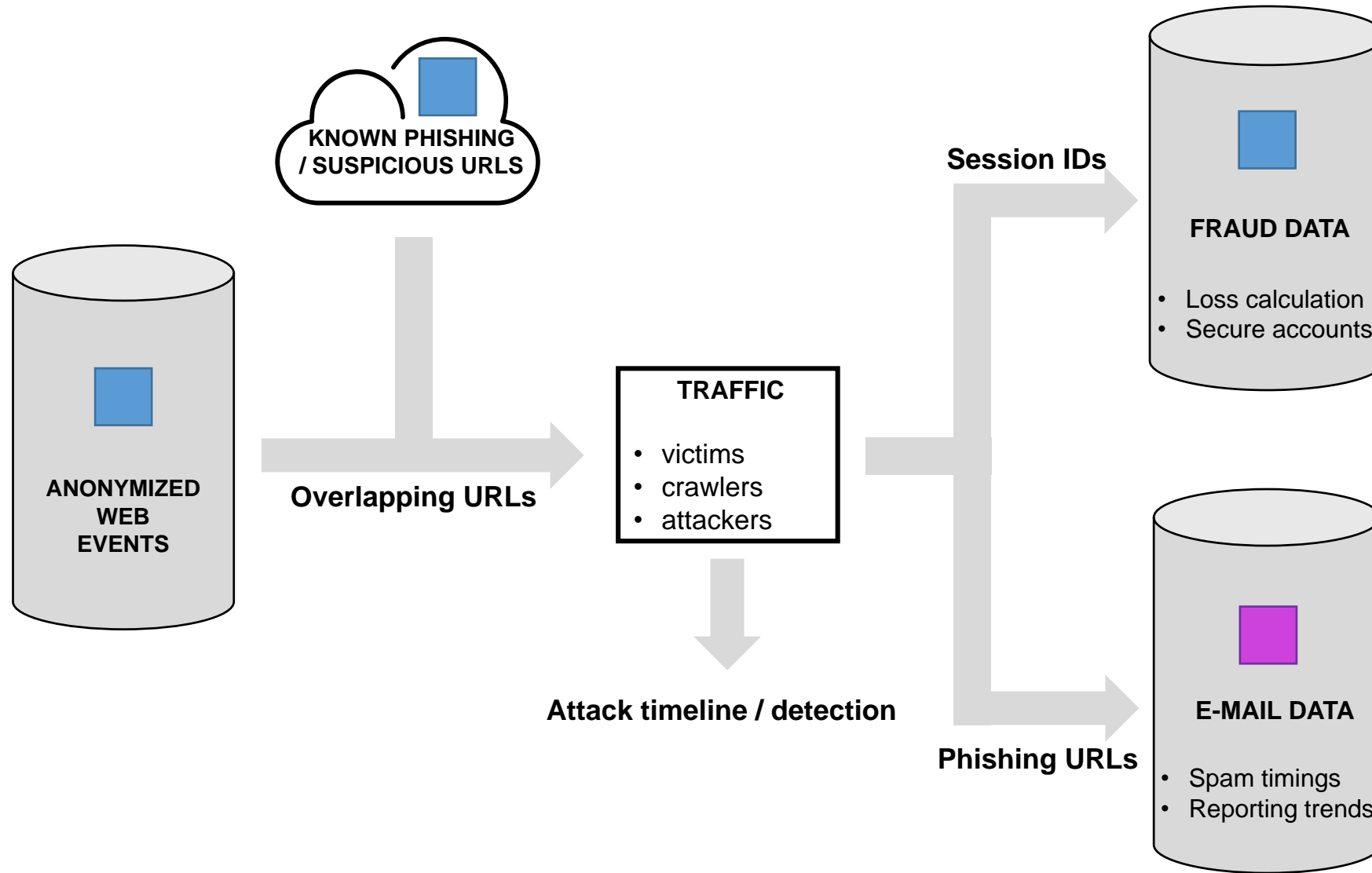
# Building an Analysis Framework

## ORGANIZATION TARGETED BY PHISHERS



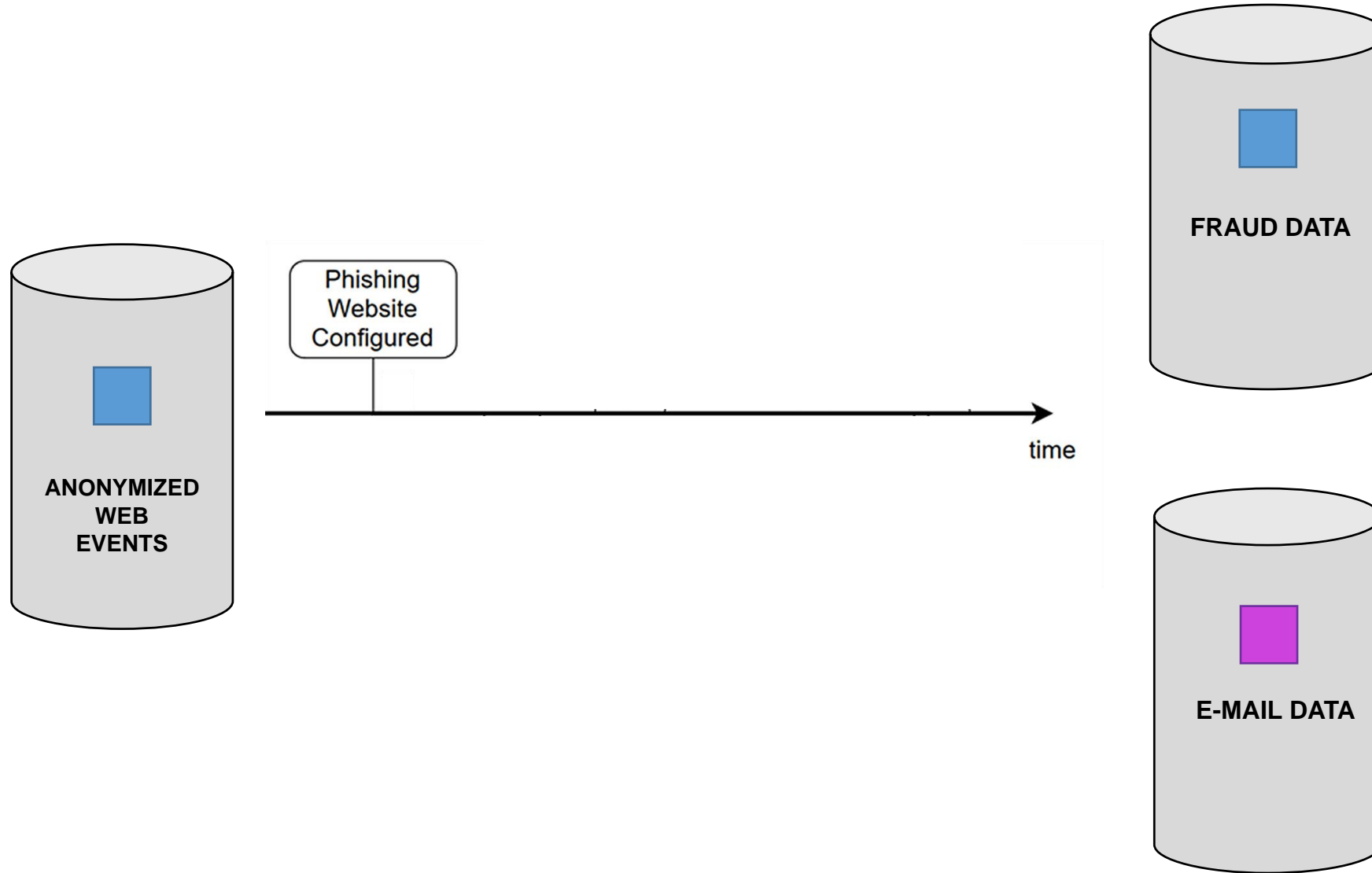
Status	Method	Domain	File	Cause	Type	Transferred	Size	0
200	GET	<del>ty364tsdsaf.appspot.com</del>	8cc47449c8e0cc4c4f254cd03568bae9nbr1570557671.css	stylesheet	css	843 B	1.06 KB	
200	GET	<del>ty364tsdsaf.appspot.com</del>	b1821919c7bcc1049302e1f2e606f003nbr1570557671.css	stylesheet	css	24.05 KB	127 KB	
200	GET	<del>ty364tsdsaf.appspot.com</del>	37_533e293f0c8947ada653b47c00e394e2.png	img	png	1.99 KB	1.71 KB	
200	GET	<del>ty364tsdsaf.appspot.com</del>	microsoft_logo.svg	img	svg	1.84 KB	3.57 KB	
200	GET	<del>ty364tsdsaf.appspot.com</del>	ellipsis_white.svg	img	svg	605 B	915 B	
200	GET	<del>ty364tsdsaf.appspot.com</del>	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



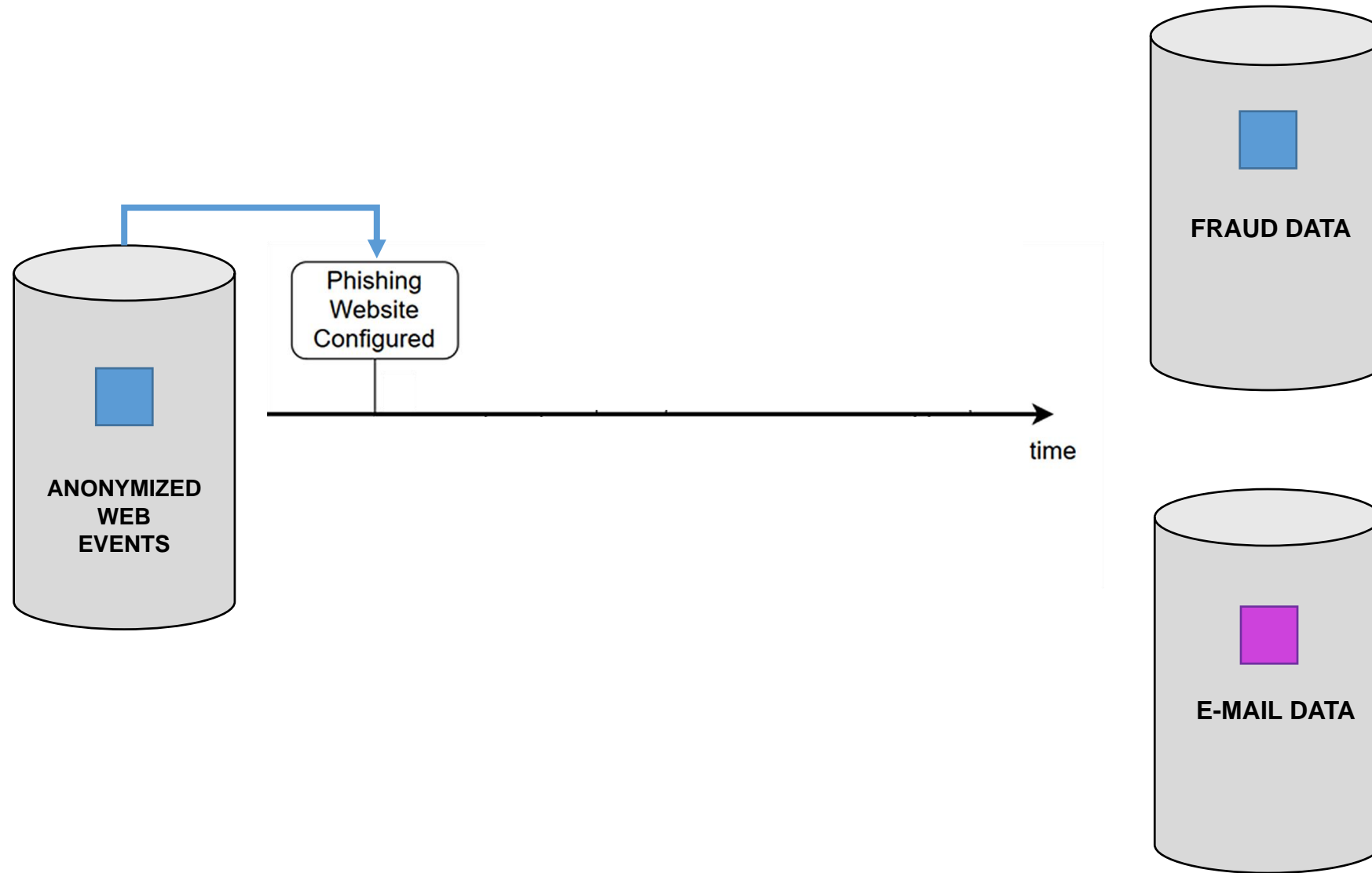
# End-to-end Timeline

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



# End-to-end Timeline

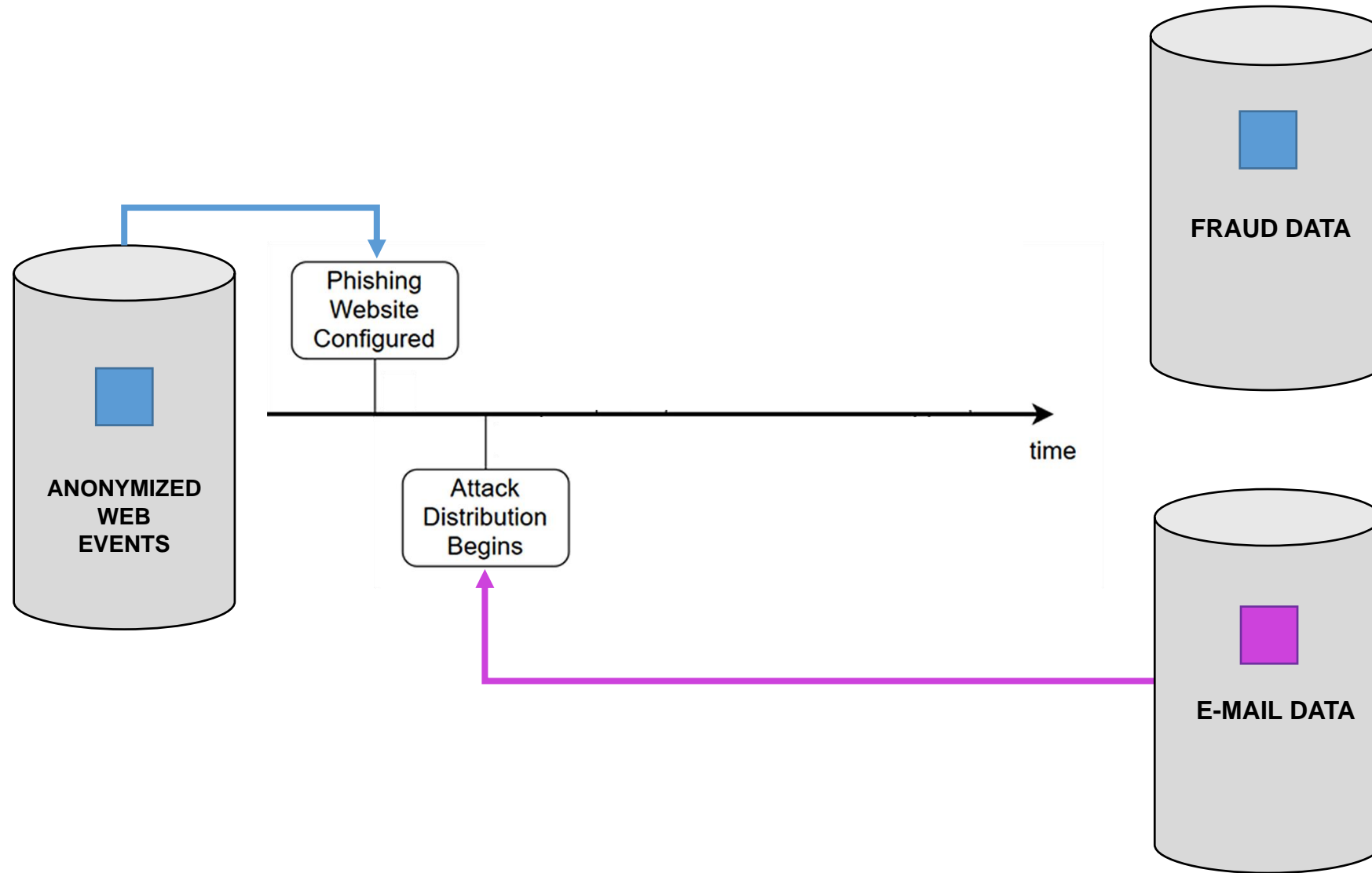
-  ORGANIZATION TARGETED BY PHISHERS
-  E-MAIL PROVIDER / PHISHING REPORTS



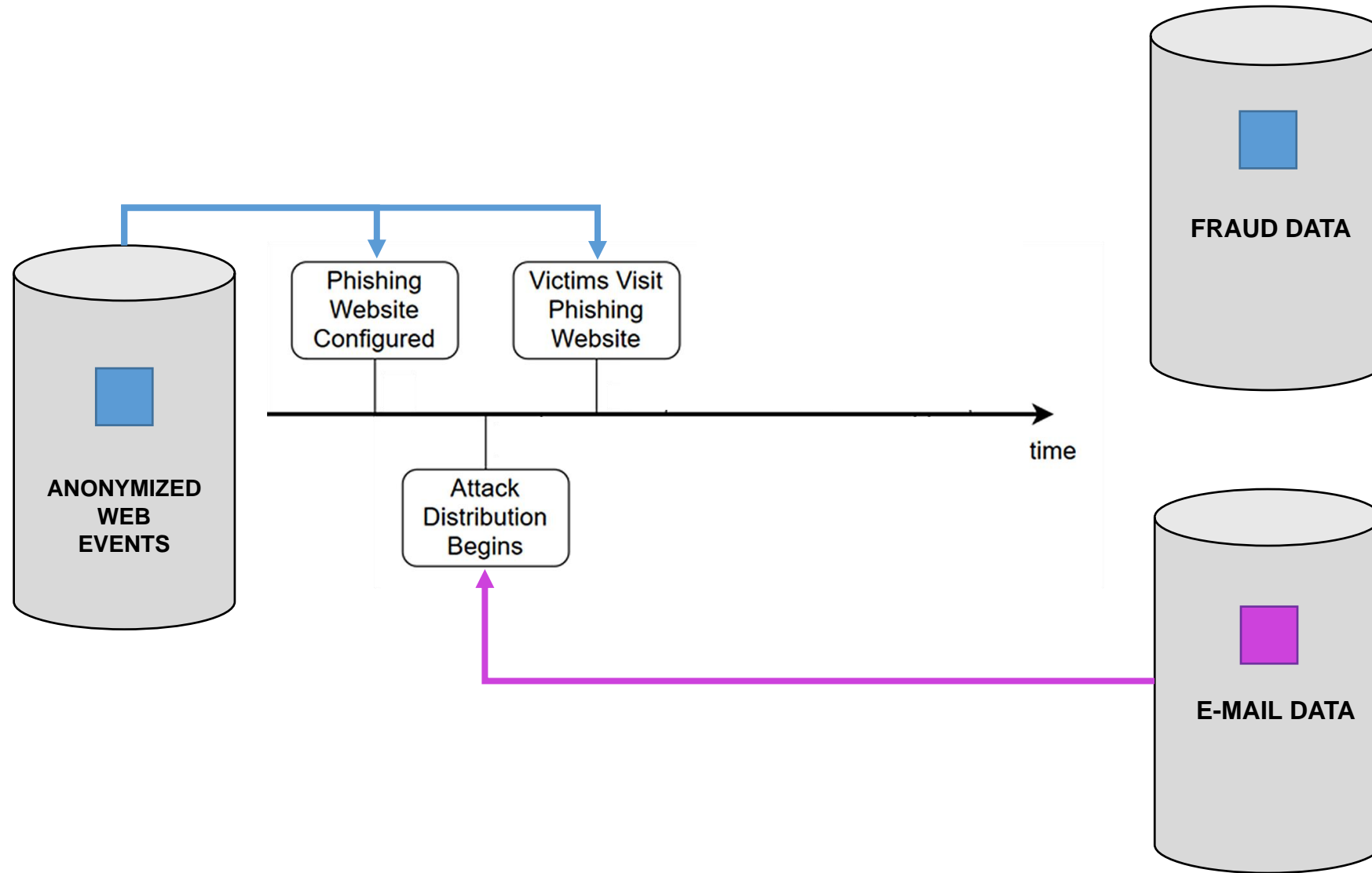


# End-to-end Timeline

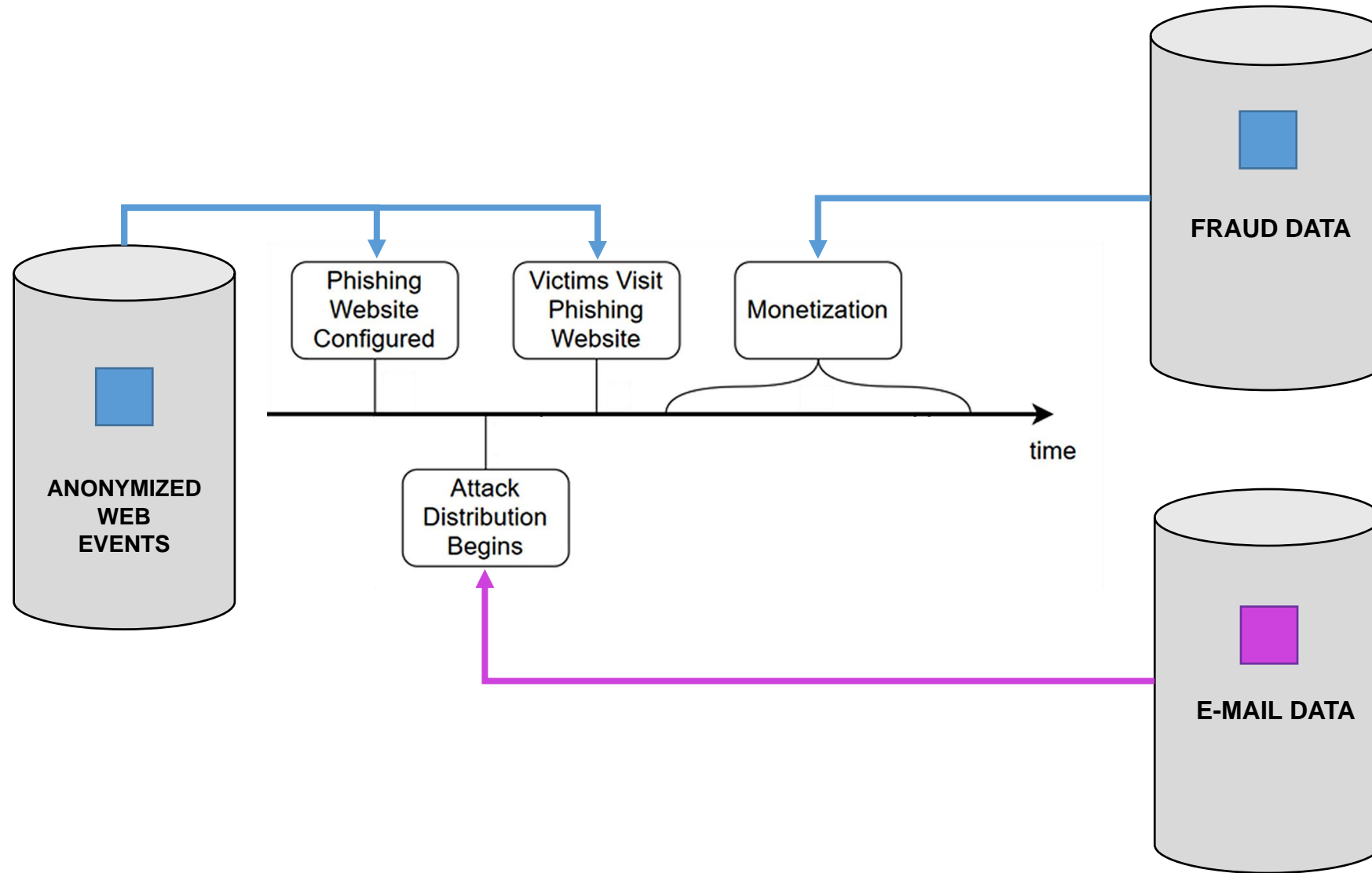
- ORGANIZATION TARGETED BY PHISHERS
- E-MAIL PROVIDER / PHISHING REPORTS



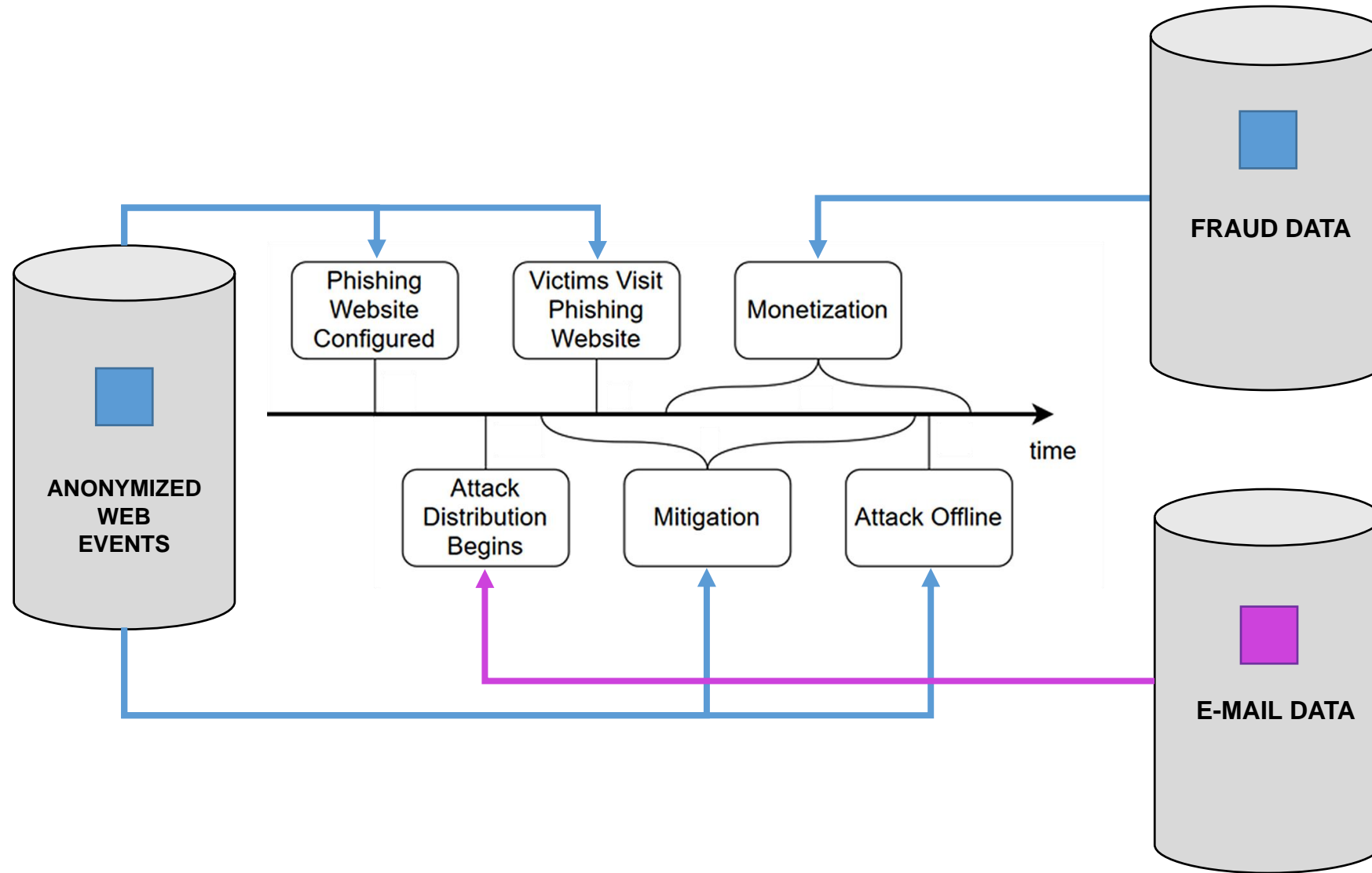
# End-to-end Timeline



# End-to-end Timeline



# End-to-end Timeline



# “Golden Hour” Data Set

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

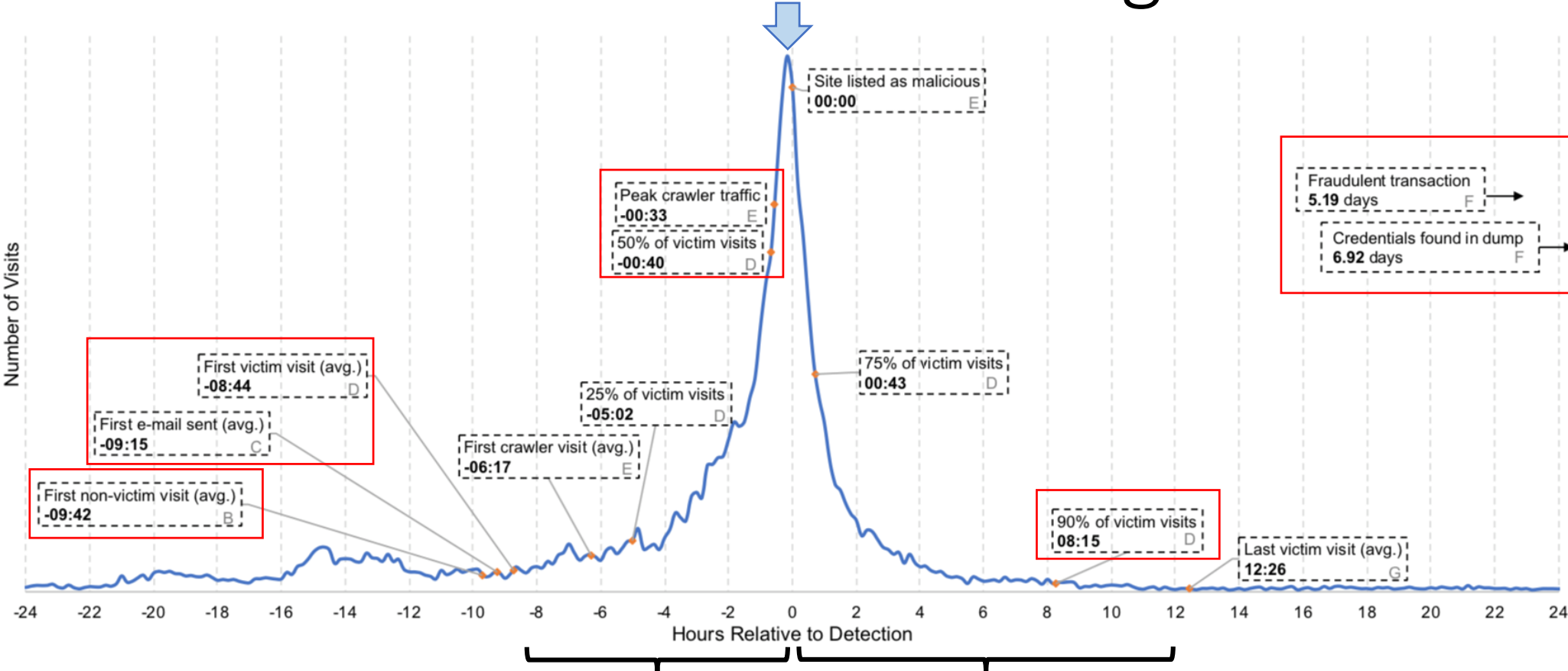


- **Visibility:** 39.1% of known phishing domains

	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



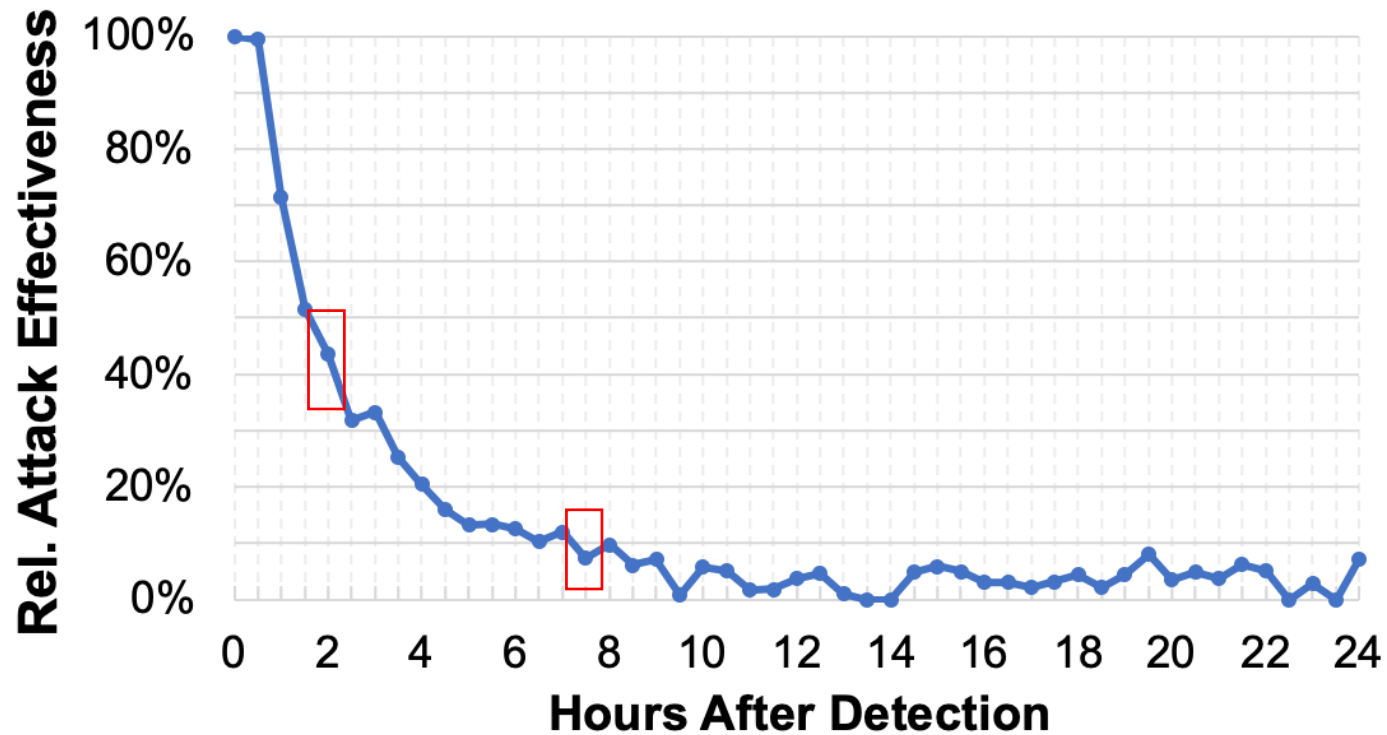
Proactive detection    Reactive mitigation improvements

Secure affected user accounts



# Estimating Browser-based Detection

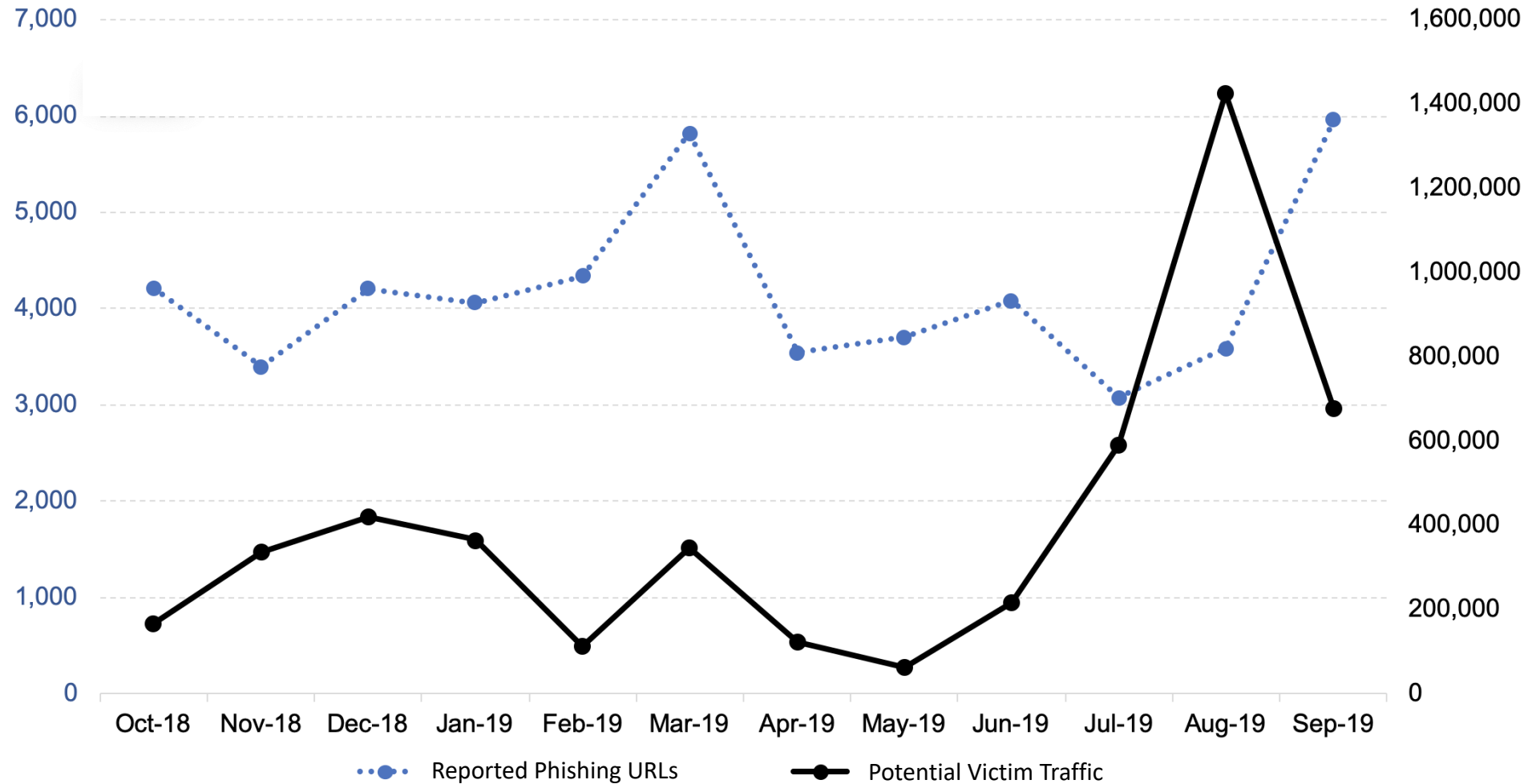
Ratio: Traffic from **browsers w/anti-phishing features** vs. **other browsers**



PhishTime: Continuous Longitudinal Measurement of the Effectiveness of Anti-phishing Blacklists

Adam Oest, Yeganeh Safaei, Penghui Zhang, Brad Wardman, Kevin Tyers, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn. 2020 USENIX Security Symposium.

# Phishing URLs vs Victim Traffic

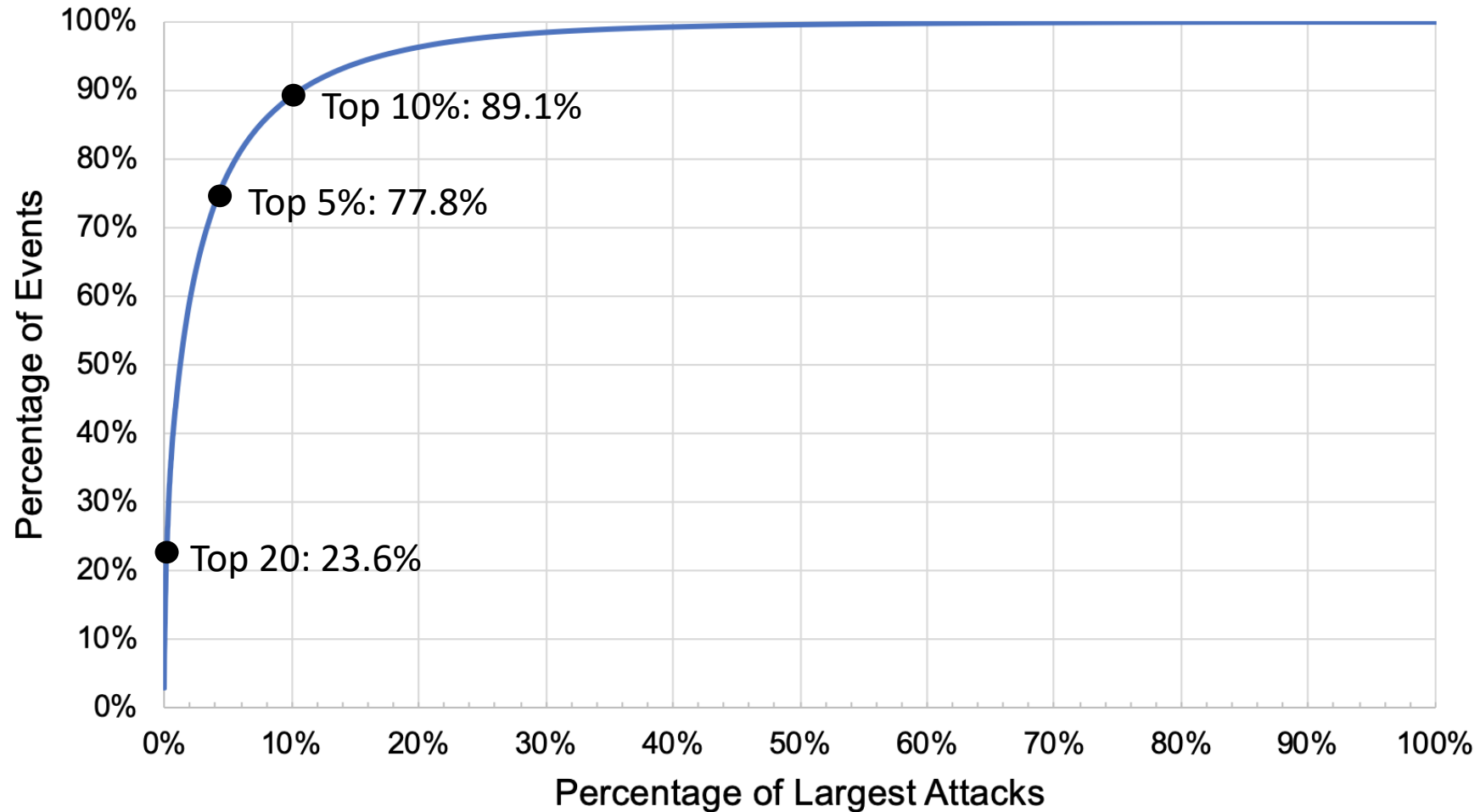




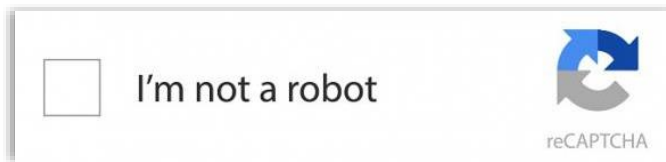
# Long-running Campaigns

Rank	First Seen Date	Last Seen Date	Campaign Duration (Days)	Known Visitor Events	Average Events Per Day	Distinct URLs Reported	URL Text Classification	Domain Type
1	01/06/2019	09/22/2019	259	145,306	560	41	Deceptive Path Only	Compromised
2	08/30/2019	09/26/2019	27	115,616	4,329	41	Deceptive Subdomain	Compromised
3	07/20/2019	09/14/2019	56	102,601	1,847	40	Non-deceptive	Free Subdomain
4	01/11/2019	01/15/2019	4	82,636	20,487	6	Deceptive Path Only	Regular Registration
5	06/14/2019	06/20/2019	6	71,478	11,681	56	Non-deceptive	Compromised
6	04/21/2019	05/27/2019	36	71,037	1,992	39	Deceptive Path Only	Regular Registration
7	08/11/2019	08/17/2019	5	59,911	11,296	40	Deceptive Subdomain	Free Domain
8	03/14/2019	04/22/2019	39	55,147	1,427	81	Deceptive Subdomain	Regular Registration
9	08/30/2019	09/26/2019	27	50,402	1,877	28	Deceptive Subdomain	Compromised
10	01/07/2019	01/07/2019	1	49,627	49,627	8	Deceptive Subdomain	Free Subdomain
11	12/22/2018	12/26/2018	4	44,502	10,806	45	Non-deceptive	Compromised
12	06/23/2019	06/28/2019	6	42,574	7,708	22	Deceptive Subdomain	Free Subdomain
13	09/24/2019	09/25/2019	2	42,406	21,203	29	Deceptive Domain	Regular Registration
14	12/12/2018	01/02/2019	21	38,484	1,814	16	Deceptive Path Only	Compromised
15	10/06/2018	02/22/2019	140	32,591	233	39	Deceptive Path Only	Compromised
16	12/11/2018	12/29/2018	18	30,983	1,768	63	Deceptive Subdomain	Regular Registration
17	10/31/2018	03/24/2019	145	30,853	213	90	Deceptive Path Only	Regular Registration
18	09/12/2019	09/22/2019	10	30,781	2,990	23	Deceptive Path Only	Compromised
19	03/19/2019	03/24/2019	4	23,552	5,399	21	Deceptive Path Only	Regular Registration
20	08/13/2019	08/15/2019	3	22,254	7,418	16	Deceptive Domain	Regular Registration

# Top Campaigns: Majority of Victim Traffic



# Bot evasion: Human Verification



# Extensive Identity Theft

Confirm Billing Address

Cardholder Name  
Bob Rob

Card type  
Visa

Credit card number  
4450 0036 2091 8442

Expiration Date  
01 / 2025

Security code  
638

Date of Birth  
10 / 10 / 2010

Phone number  
4804444444

Address  
Pheonix Avenue

City  
Lowell

Zip code  
01852

State  
Massachusetts

Country  
United States of Am...

Confirm

HELP & CONTACT

Policy updates Feedback

# Extensive Identity Theft

○ ○ ● ○


## Confirm your identity

Your identification documents will help us to validate your identity.

What i should to do, to confirm my identity?

- Take a selfie by holding your ID Card also your Card
- Cardholder Name and ID Card should match and be clearly visible.
- Your identification document must be next to your face.

Here's an example for picture :



✓ CORRECT      ✗ INCORRECT

Choose files To Upload

By clicking Agree & Continue, I have read and agree to [User Agreement](#), [Privacy Policy](#) and [Electronic Communications Delivery Policy](#).

# Convincing Victims: Automatic Translation

## クレジットカード決済を、 ペイパルでかんたん＆安心に。

ペイパルは、いままでにないオンライン決済サービスでショッピングとビジネスの未来をカタチにするイノベーターです。時代のニーズに合わせた、よりかんたんで安心な決済サービスを提案し、世界中のショッピングとビジネスをシンプルに変えていきます。

[新規登録はこちら](#)

重要なお知らせ：ペイパルを装った不審な電子メールにご注意ください。

# Victim Reassurance

## Your Account Access is Fully Restored

Thank you for taking the steps to restore your account access. Your patience and efforts increase security for our entire community of users.

[My Account](#)

# Conclusions

- End-to-end look at large-scale phishing attacks
  - Prioritizing mitigation of sophisticated phishing
- Golden Hour system deployed at major organization
  - Securing user accounts
  - Proactively discovering malicious URLs
  - Tracking COVID-19 phishing campaigns
- Future work
  - Collaborative, cross-organizational framework
  - Incorporation of signals beyond web requests





# Thank you!



**Adam Oest**  
aoest@asu.edu