Registration, Detection, and Deregistration: Analyzing Lifecycles of Phishing Attacks

Kyungchan Lim, Raffaele Sommese, Mattijis Jonker,
Ricky Mok, KC Claffy, Doowon Kim

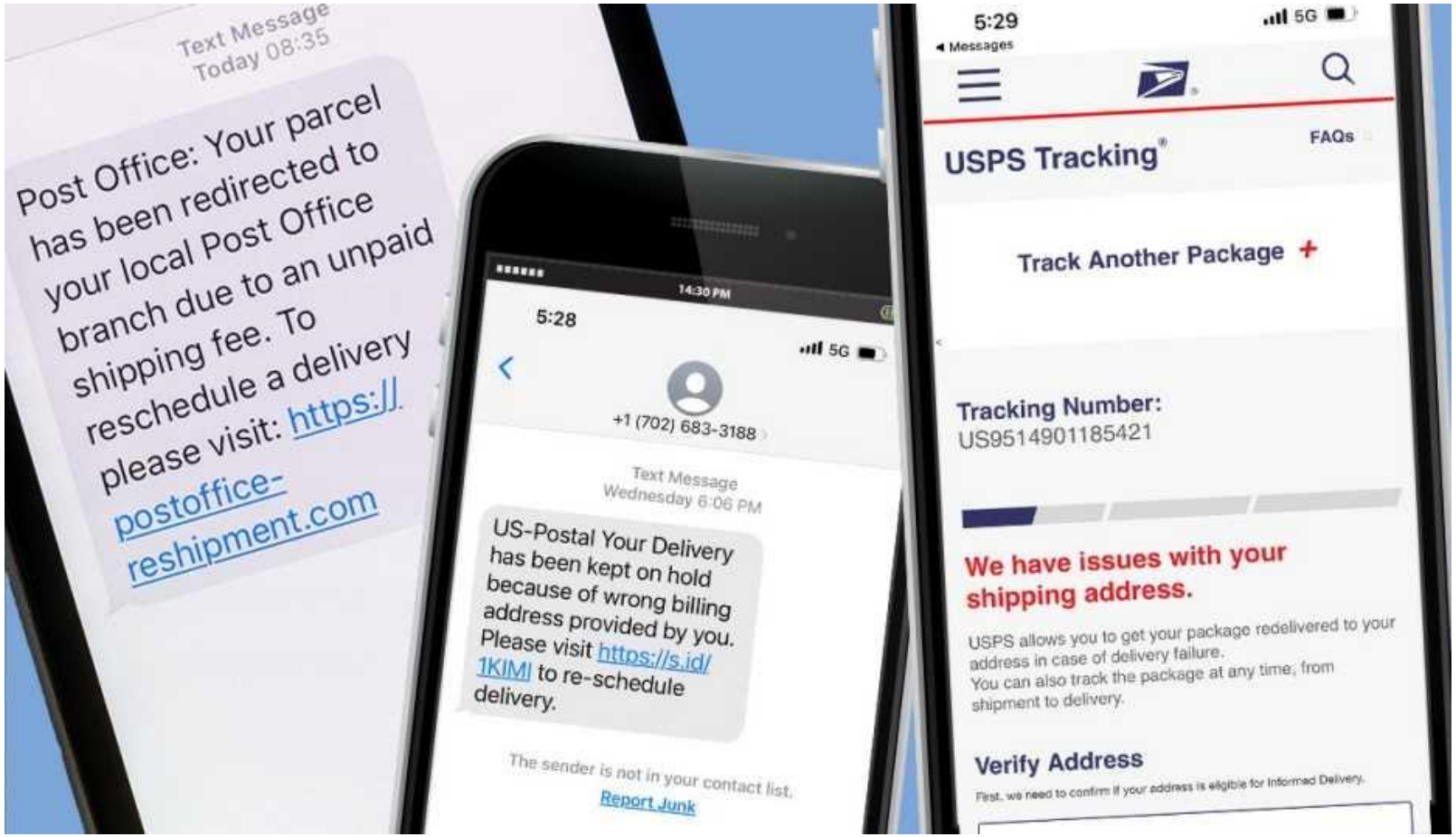
ICANN SSAC Lightning Talk

9 March 2025

THE UNIVERSITY OF TENNESSEE KNOXVILLE

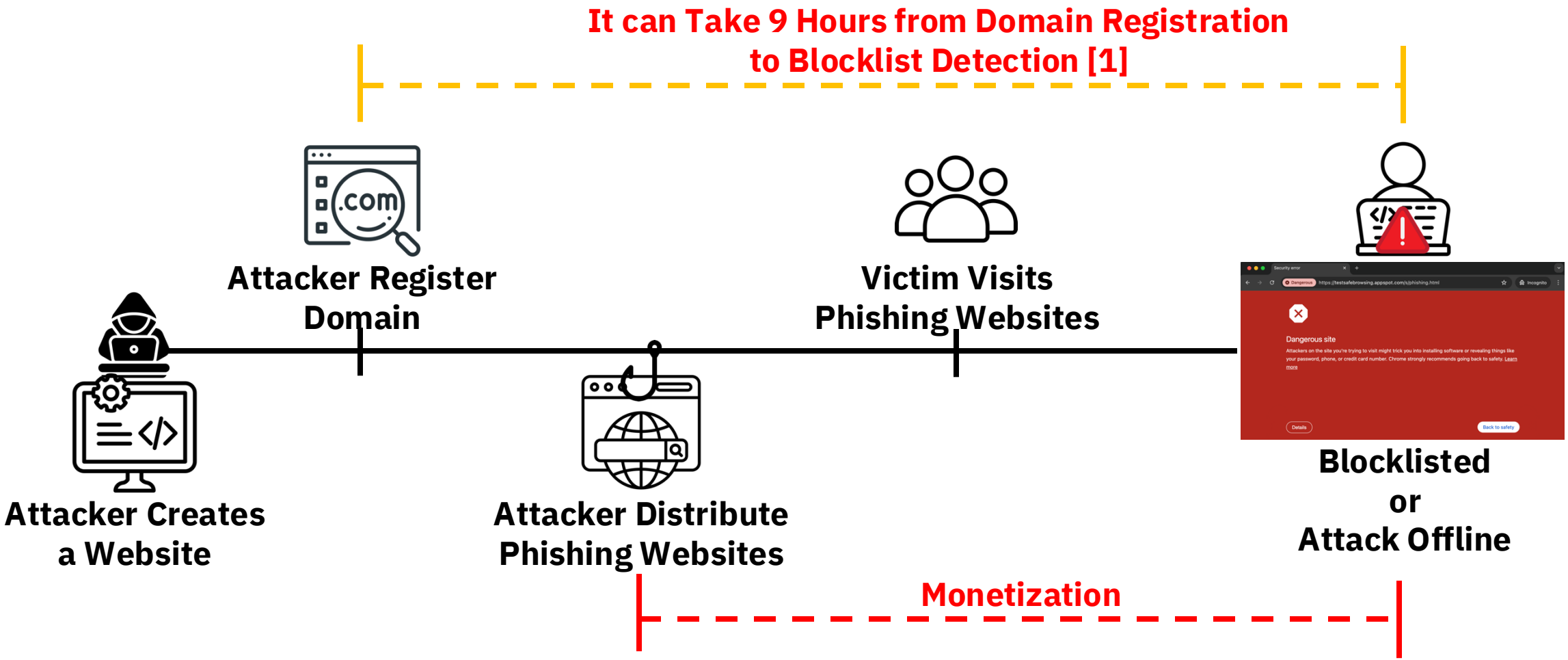
Motivation: Continued Growth of Phishing Attacks

- New(er) phishing attack vector: urgent text message!



[1] https://www.aarp.org/money/scams-fraud/fake-usps-ups-smishing-texts/

Life Cycle of Phishing Attacks



[1] Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale, USENIX 2020

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Blocklisting: Popular but Problematic

- **Blocklisting** is a **popular** defense method
  - Google Safe Browsing → Provides defensive action by **warning** users before browser **accesses malicious website**
  - Many blocklists
    - APWG, VirusTotal, PhishTank, OpenPhish, etc

However, blocklisting has limitations

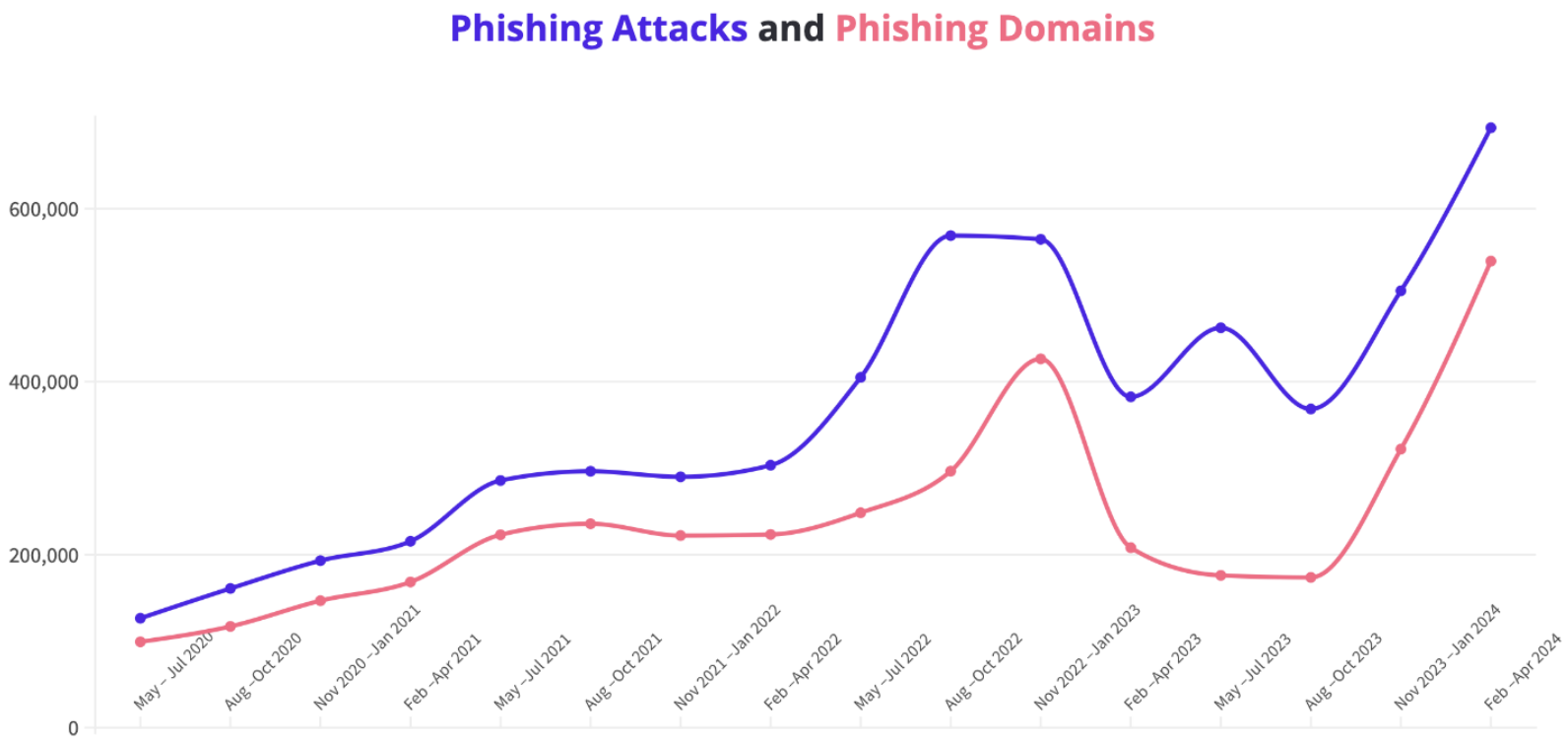
Blocklisting: Popular but Problematic

Blocklist limitations:

- Delayed Response: Blocklists require time to analyze and classify potentially malicious websites, creating a window of vulnerability
- Inconsistent Detection Methods: Each blocklist uses proprietary detection techniques that vary in sensitivity and coverage
- Diverse Data Sources: Detection relies on different methodologies:
  - Community-driven reports (PhishTank, OpenPhish)
  - Active scanning systems (Google Safe Browsing)
- Variable Accuracy: Community-driven approaches may produce higher false positives, while service-provider blocklists like Safe Browsing tend to be more conservative with fewer detections
- Lack of Standardization: The absence of unified standards across blocklists creates gaps in protection and complicates integration

Research Goal: Detect Phishing Domains Early

- Identify characteristics of malicious domains, to increase chance of identifying phishing before it launches



- Interisle's report [1] uses APWG, OpenPhish, PhishTank, Spamhaus
- They infer malicious domains based on:
  - Age: Domains with lifespans less than one year
  - Deliberate misspellings of established brands
  - Visual similarity to legitimate brands

[1] https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing

How Far Have We Come?

- **Industry stakeholders: APWG** [1], **Interisle** [2], and **Netbeacon** [3] have characterized **increases in phishing attacks**
- Researchers have developed techniques for **identifying malicious (vs compromised) domains** [4,5,6]
- Our goal: **reproduce** research with **reproducible datasets** and **provide updated findings** on our real-world phishing dataset

[1] apwg.org/trendsreports/
[2] interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing
[3] netbeacon.org/phishing-attack-trends-2/
[4] Maroofi et al., COMAR: Classification of Compromised vs Maliciously Registered Domains, Euro S&P, 2020
[5] Moura et al., Characterizing and Mitigating Phishing Attacks at ccTLD Scale, CCS, 2024
[6] Lim et al., Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks

Report / Paper	Type of Data	Time Range	Key Findings
APWG Report [1]	URL Reports (APWG)	Quarterly 2024 Q3	1. Phishing increased, reaching near-record levels. 2. Emphasized broad phishing activity against financials and delivery services. 3. Identified different targeted sectors and scam types.
Interisle Report [2]	APWG, OpenPhish, PhishTank, Spamhaus, Zone file, WHOIS, RDAP	Yearly 2024	1. Phishing increased sharply, especially in new gTLDs (42% of phishing domains). 2. Top TLDs for phishing: .com, .top, .xyz (maliciously registered) and .com, .net, .org (compromised). 3. Interisle counts each URL as a separate attack (URL-based counting).
NetBeacon Report [3]	Registrars, Abuse reports	Yearly 2024	1. Phishing increased early in 2024. 2. Most malicious domains were registered at a small group of registrars. 3. Undercounting phishing attacks on multi-tenant platforms.
COMAR [4]	OpenPhish, PhishTank, URLhaus, WHOIS, RDAP, TLS data	2019/03 – 2019/07	1. Distinguishes compromised vs maliciously registered domains with claimed 97% accuracy (validated against APWG lists). 2. Lexical and content-based features critical. Minimal content on malicious domains. 3. 12% of domains are compromised w/in 3 months of registration.
Characterizing and Mitigating Phishing Attacks at ccTLD Scale [5]	ccTLD (.nl, .be, .ie) Blocklists (Netcraft)	10 Years (2024 – 2024)	1. Most phishing in these 3 ccTLDs used compromised domains (80%). 2. National brands targeted with newly registered ccTLD domains. Global brands targeted using compromised domains. 3. Phishers adapt to language and trust environment of target country.
Our Work [6]	APWG, DNS records, WHOIS, RDAP, CT logs, Zone files	39 Months (2021/07 – 2024/10)	1. 66% of phishing domains maliciously registered, detected faster than compromised ones. 2. New gTLDs (e.g., .top, .xyz) dominate malicious registration, com/net dominate compromised. 3. Counted 2LD but tracked some changes at subdomain/brand level.. Blocklisting granularity varies (mostly URL-based).
	OpenPhish, PhishTank, Malware-filter, Phishing.Database, phishunt.io,	5 Months (2024/05 – 2024/10)	

[1] https://apwg.org/trendsreports/
[2] https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing
[3] https://netbeacon.org/phishing-attack-trends-2/
[4] Maroofi et al., COMAR: Classification of Compromised versus Maliciously Registered Domains, Euro S&P, 2020
[5] Moura et al., Characterizing and Mitigating Phishing Attacks at ccTLD Scale, CCS, 2024
[6] Lim et al., Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks

Common Findings	Report / Paper
Phishing is increasing (both in volume and sophistication)	All 6 studies
New gTLDs are **heavily exploited** for **malicious domains**	Interisle [2], COMAR [4], Our work [6]
Compromised domains still large part of problem, **especially in ccTLDs**	COMAR [4], Characterizing and Mitigating Phishing Attackers at ccTLD Scale [5]
.com remains the top TLD for phishing (due to sheer size)	Interisle [2], Our work [6]
Phishers shift TLD preferences based on **pricing** and **enforcement changes** (e.g., Freenom TLD decline)	Interisle [2], Our work [6]
Bulk registrations are **common** for **malicious domains**	Interisle [2], COMAR [4], Our work [6]

[1] https://apwg.org/trendsreports/
[2] https://interisle.net/insights/phishing-landscape-2024-an-annual-study-of-the-scope-and-distribution-of-phishing
[3] https://netbeacon.org/phishing-attack-trends-2/
[4] Maroofi et al., COMAR: Classification of Compromised versus Maliciously Registered Domains, Euro S&P, 2020
[5] Moura et al., Characterizing and Mitigating Phishing Attacks at ccTLD Scale, CCS, 2024
[6] Lim et al., Registration, Detection, and Deregistration: Analyzing DNS Abuse for Phishing Attacks

Data Sources

- Dataset: Phishing Domains from blocklists (APWG, etc)

Type	Time Range	# of URLs	# of Domains	# of TLD
APWG	39 Months (2021/07 – 2024/10)	**2,184,835**	**697,237**	**1,203**
phishunt.io	5 Months (2024/05 – 2024/10)	262,755	66,743	598
PhishStats		221,331	57,299	541
OpenPhish		115,804	26,127	480
Malware-filter		76,465	24,300	470
PhishTank		5,579	1,695	195
Phishing.Database		363	236	51
Total (Distinct)	-	2,294,267	765,910	1,258

Approach/Method

- From phishing domains, how can we identify malicious domains?

Identify Maliciously-registered Domains

- Using our APWG phishing domain list:
  - **Identify maliciously-registered domains** with 4 types
  - 66.1% of domains in our dataset are malicious
  - Rest (=33.9%) compromised

Type	# of Domains	Examples
Brand Name in Domain	35.9%	www.usps-security-login.com
Squatted Domain	26.2%	facebo0k.com
Random-looking Domain	28.2%	urpxu.com, urpzi.com
Bulk-registered Domain	7.9%	rbcwealthmanagement.com, rbcwealthmanagement.com
Total	66.1%	

Characteristics of Malicious Domains

- What kind of characteristics do malicious domains have?
  - TLD Usage
  - Targeted Brand
  - Lifespan

Which TLDs do Malicious Domains Use?

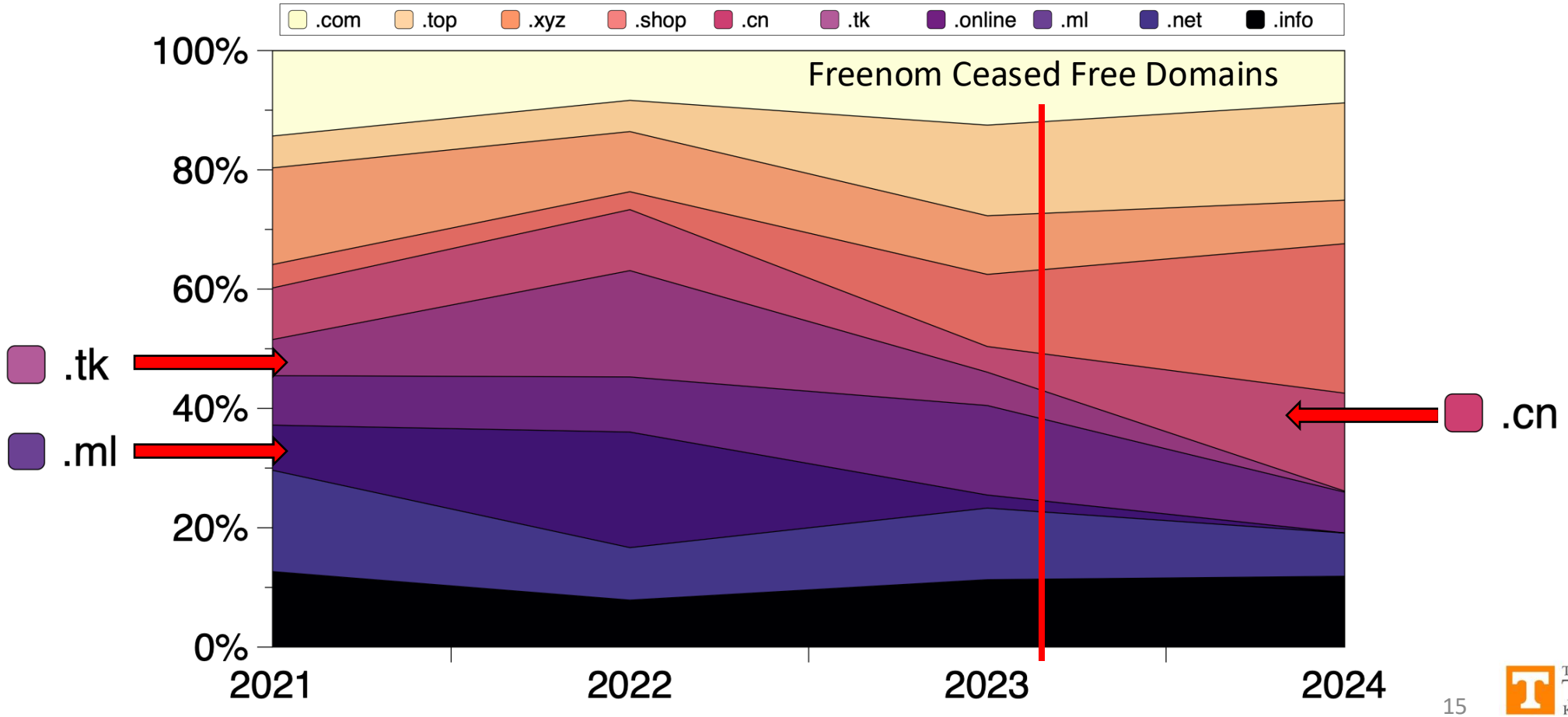
- From malicious domains in APWG list of phishing domains:
  - Attackers tend to use cheaper TLDs (new gTLDs, via Freenom registrar)

TLD	Price	Maliciously Registered Domains	Compromised Domains
.com	$6	65.28%	34.72%
.top	$1	63.78%	36.22%
.xyz	$1	61.24%	38.76%
.shop	$1	68.32%	31.68%
.cn	$5	80.86%	19.14%
.tk	$7	60.41%	39.59%
.online	$1	59.98%	40.02%
.ml	$12	71.53%	28.47%
.net	$10	63.83%	36.17%
.info	$2	76.49%	23.51%

THE UNIVERSITY OF TENNESSEE KNOXVILLE

TLD Usage Over Time in Phishing Domains

- From malicious domains from APWG phishing domains between 2021 and 2024:
  - Freenom TLD usage reduced to almost none after 2023
  - .cn increase over time



Which Brands do Malicious Domains Target?

- APWG lists targeted brands for each reported phishing domain
- We analyze the most targeted brands and how they utilize different TLDs
- We use brand information provided by APWG

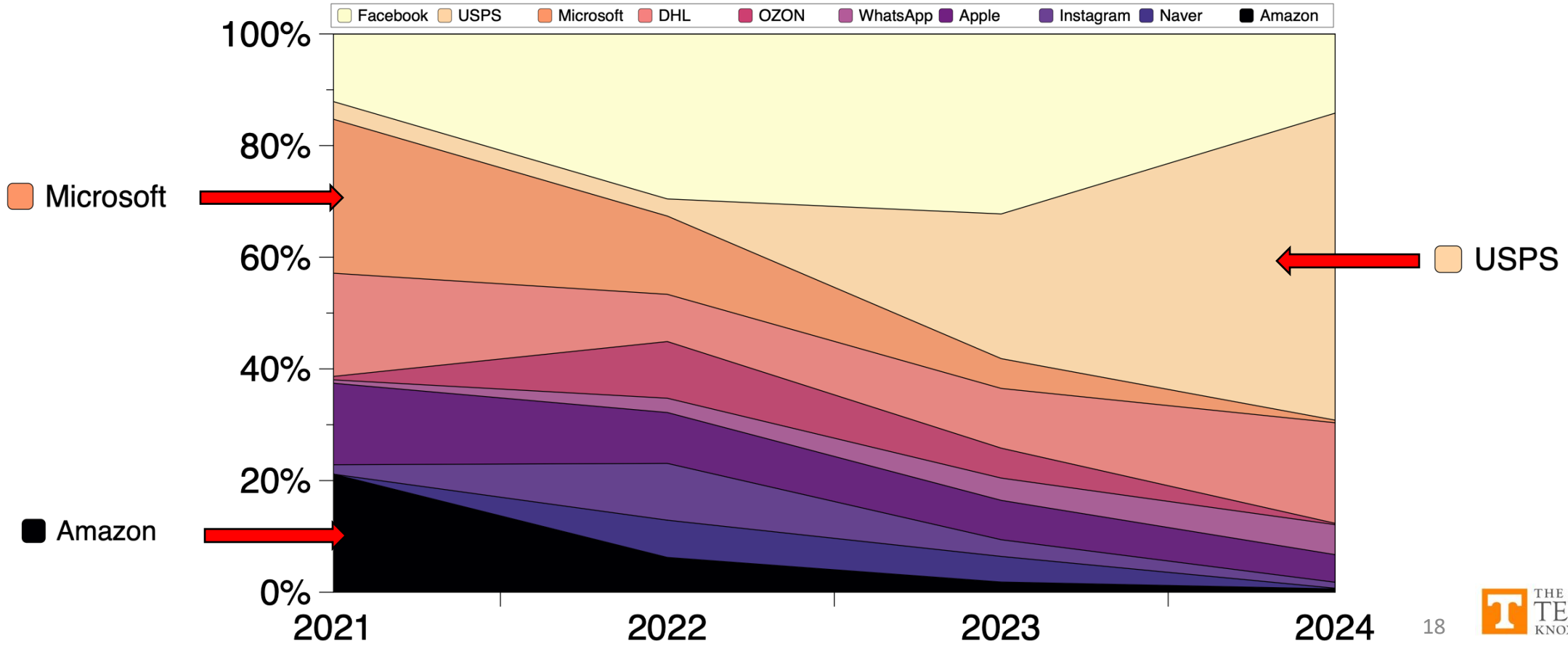
Targeted Brands in Phishing Domains

- For certain targeted brands, attackers use different TLDs than original (brand's) TLD

Brand	Country	# of Malicious Domains (%)	Dominant TLD	Original TLD
Facebook	US	58.2%	.com	.com
USPS	US	90.0%	.top	.com
Microsoft	US	51.2%	.com	.com
DHL	GER	67.1%	.com	.com
OZON	RUS	55.4%	.tk	.ru
WhatsApp	US	71.7%	.com	.com
Apple	US	79.5%	.com	.com
Instagram	US	65.6%	.ml	.com
Naver	KOR	65.3%	.com	.com
Amazon	US	78.0%	.com	.com

Targeted Brand Over Time in Phishing Domains

- Phishing targeting USPS increases, especially after 2022
- Phishing targeting Microsoft and Amazon decreases in both malicious and compromised domains

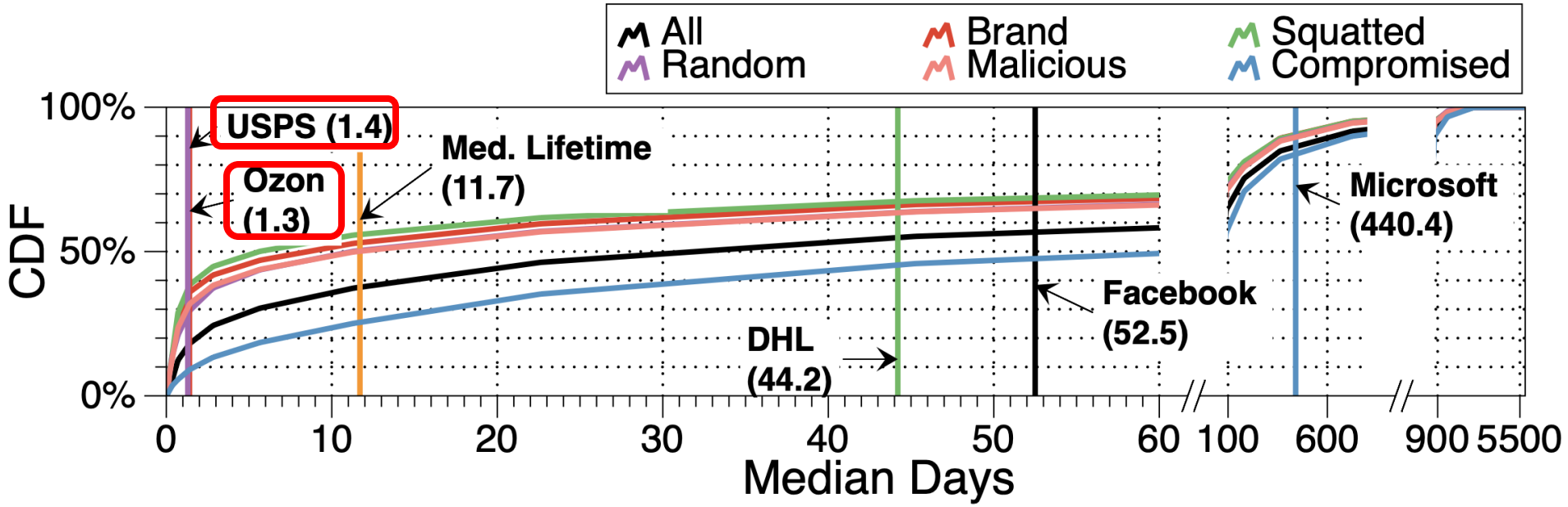


Analyzing Lifespan of Malicious Domains

- From registration to detection

Lifespan of Maliciously-registered Domains

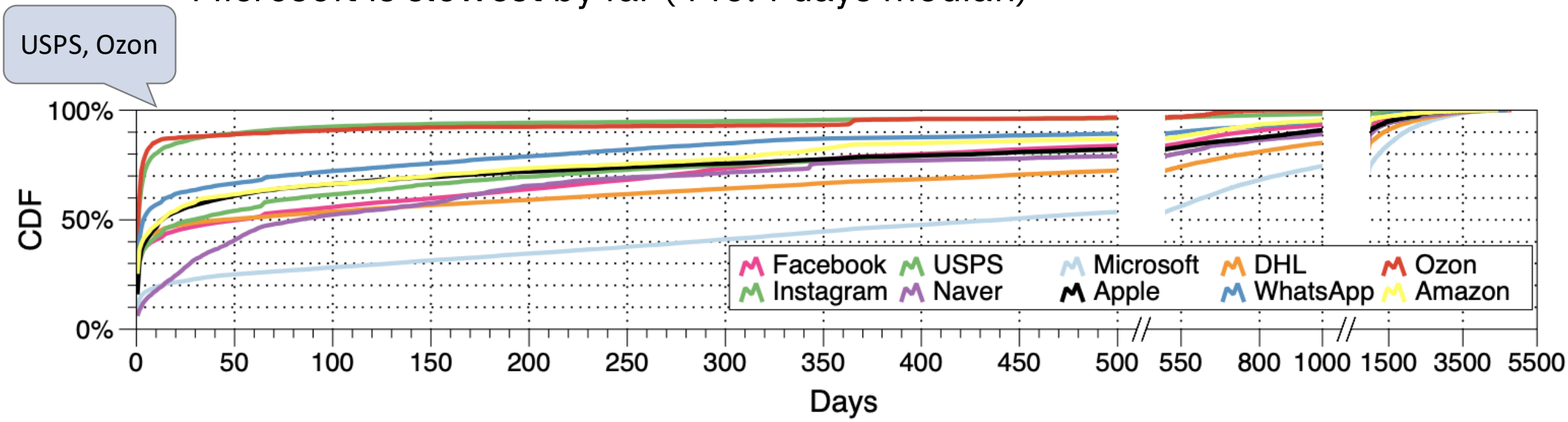
- Malicious domains detected earlier than compromised
  - 16.3 vs. 86 days
- USPS and Ozon phishing detected earlier than other brands



Median Delays (days) Between Registration and Detection

Lifespan from Registration to Detection

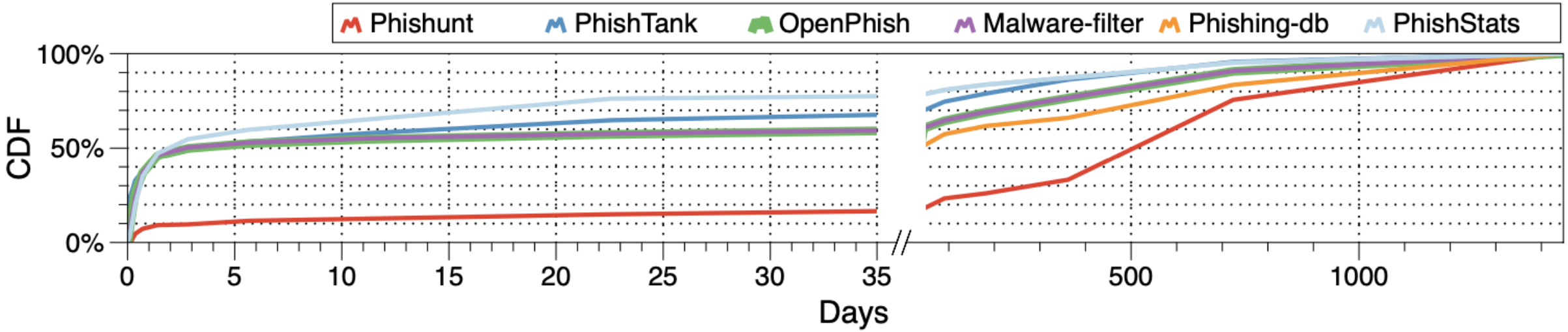
- Attacks on USPS and Ozon detected early (1.4 and 1.3 days median)
  - For Ozon, many attacks use .tk, which has APIs for immediate report
  - Microsoft is slowest by far (440.4 days median)



Days Between Registration and Detection by Top 10 Brand

Comparting Detection Speed

- Among different blocklists, APWG detects the quickest
- Other list exhibit noticeable detection delay



Days Between APWG Detection and Other Blocklists

Future Directions

- **Goal: Identify attacker characteristics by analyzing DNS features of malicious domain, then detect an attacker**
  - Analyze TLD migration and infrastructure changes
    - How attackers shift from cheap TLDs to ccTLDs or vice versa.
  - Infrastructure sharing across phishing campaigns
    - IP infrastructure, name servers, registrars
  - Comparison with benign domain for DNS records (e.g., TTL)
  - How attackers utilize bulk registration for their attacks

Conclusion

- Phishing attackers **tend to use cheaper TLD** to register malicious domains
- **Instead** of **using the original TLD** (e.g., .com, .ru) used in the targeted brand domain, attackers **use different TLD** (e.g., .top, .tk)
- By **different** targeted **brands**, **detection** speed **differs**
- **Target brand changes** (i.e., increase of USPS phishing)
- Preliminary draft: https://arxiv.org/abs/2502.09549
  - (comments welcome!)

Questions?

Kyungchan Lim

klim7@utk.edu