Department of Computer Science

Examining Newly Registered Phishing Domains at Scale

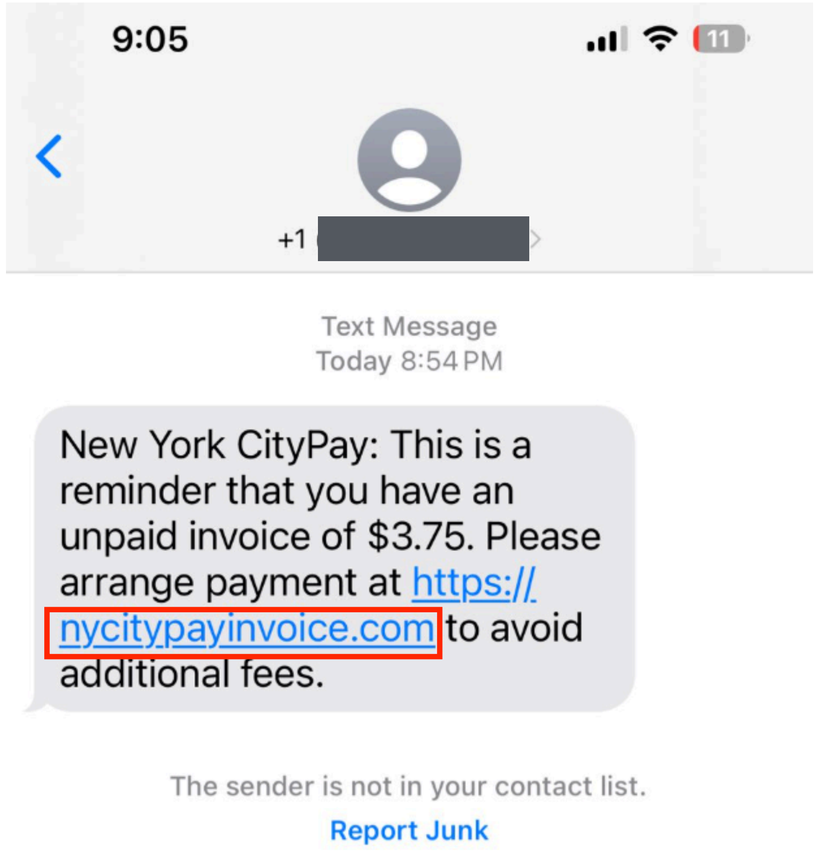
Sharad Agarwal and Marie Vasek

Workshop on Economics of Information Security (WEIS'25)

25th June 2025

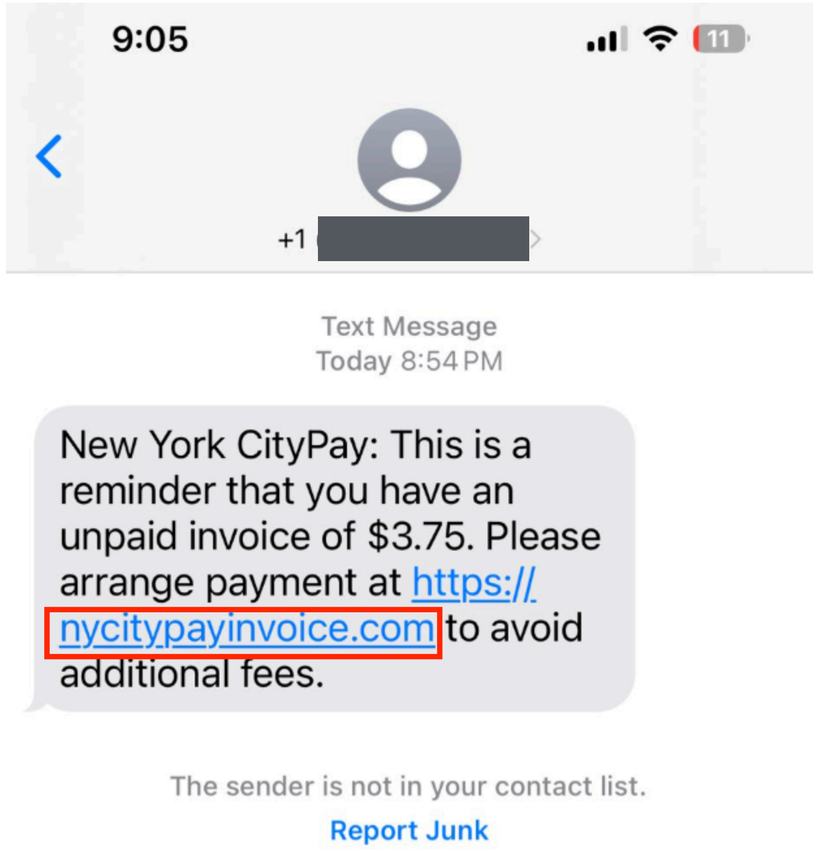
sharad.agarwal@ucl.ac.uk

Smishing abuses newly registered domains



* https://www.silentpush.com/blog/imp-1g-smishing/

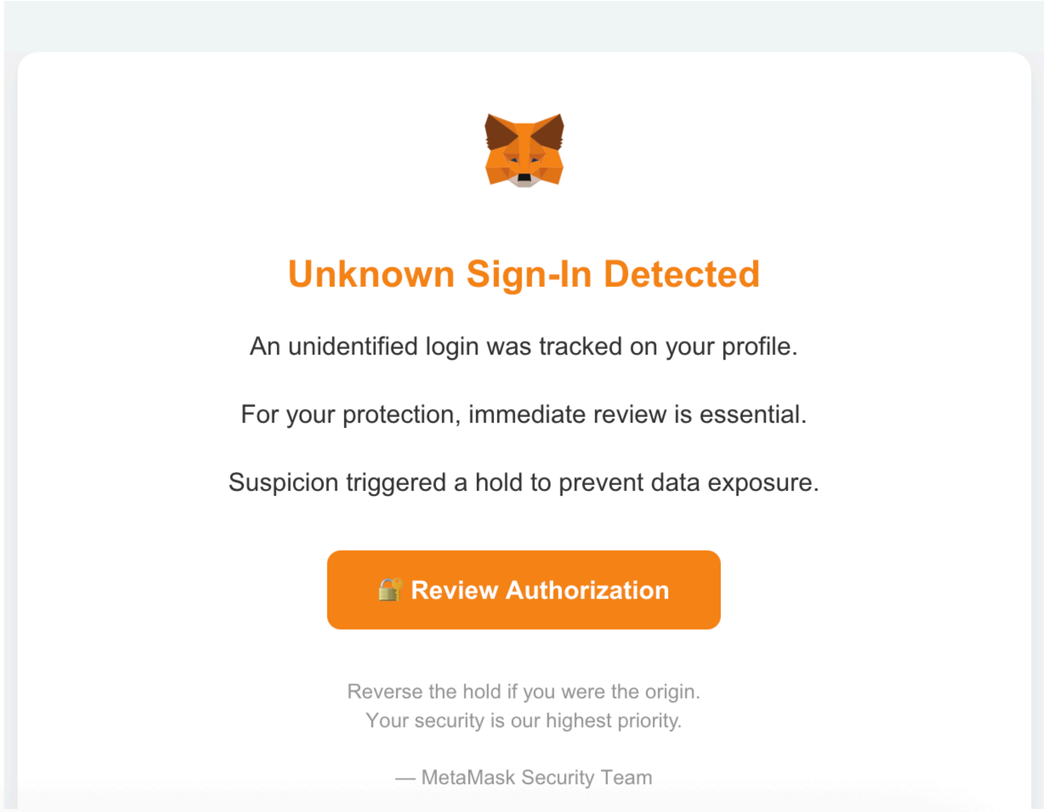
Current smishing landscape



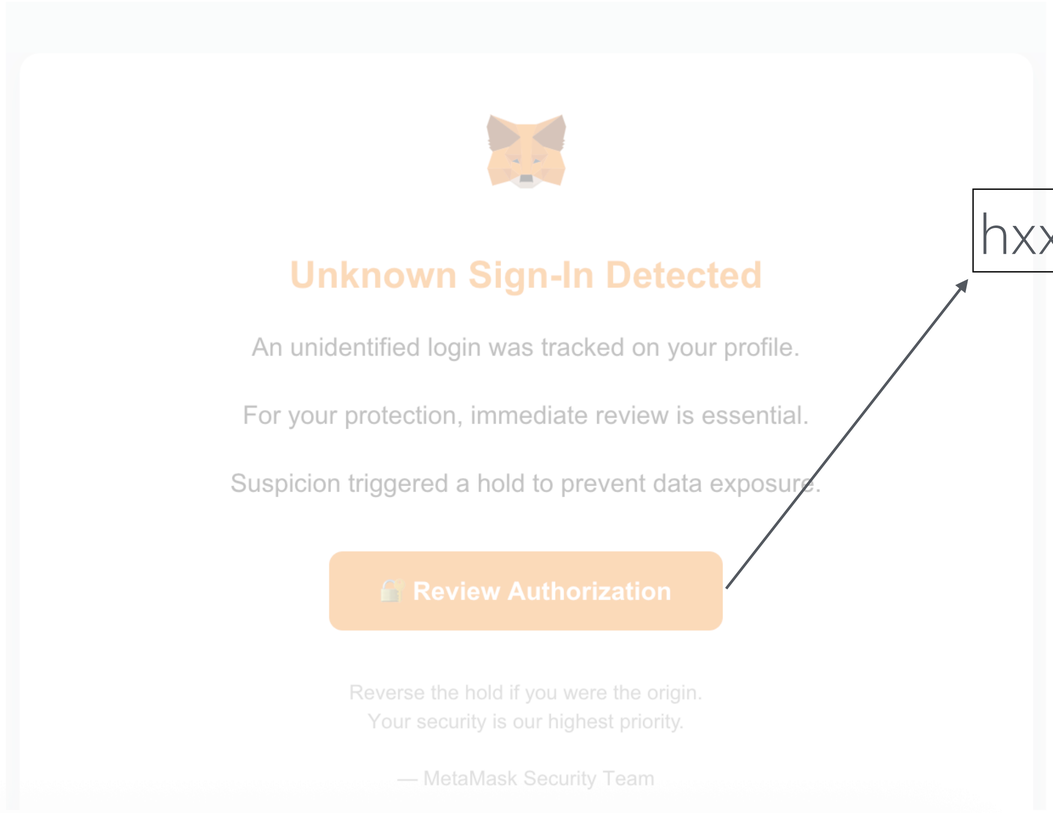
- Proofpoint's yearly report shows smishing attacks have significantly increased over the years.
- US FTC reports $470 million loss to text scams with $129k just towards Toll Scams in 2024.[1]
- Over 3.58m flagged SMS texts targeted over 2.23m mobile numbers of users of one UK MNO in two months.[2]

[1] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/04/top-text-scams-2024
[2] Agarwal, S., Harvey, E. and Vasek, M. 2024. Poster: A Comprehensive Categorization of SMS Scams. In Proceedings at ACM IMC 2024.

Adversaries compromise legitimate domains for phishing emails



Obfuscated URL in phishing emails redirect to hacked domain



Obfuscated URL

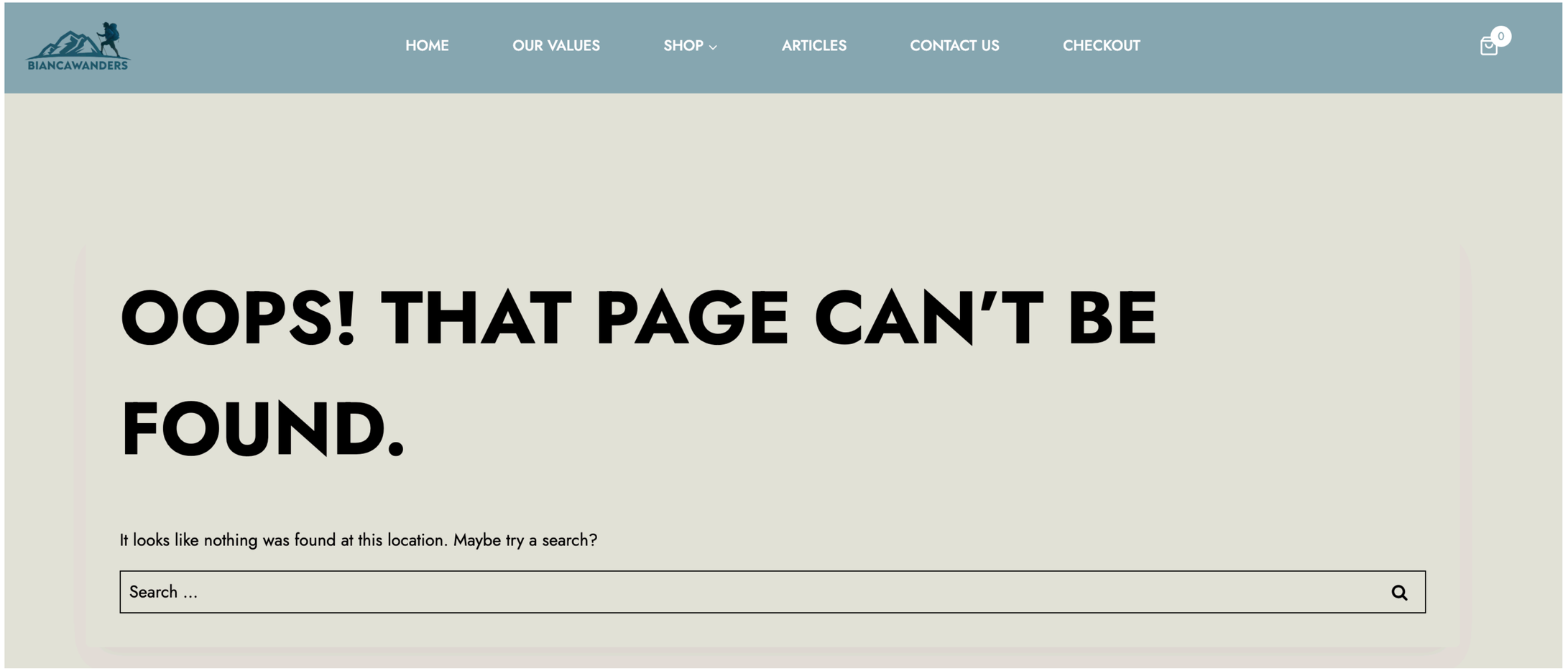
hxxps://t[.]co/Pg0OlQOKRU?id=389244171889527 4016-3107

Redirects to

hxxps://biancawanders[.]com/apple/

Compromised domain hosting a phishing webpage

The phishing webpage was hosted on this legitimate website



Newly registered phishing domains

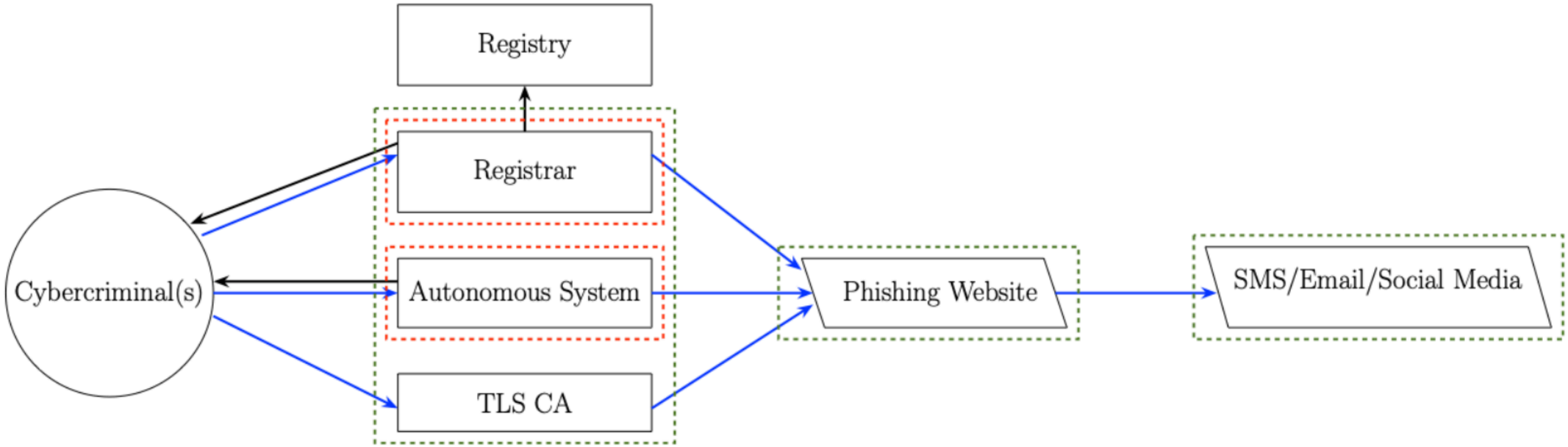


Figure 3: Cybercriminals register a new domain solely intending to host phishing. Black lines: user activities and stakeholder interactions. Blue lines: cybercriminal activities. Green boxes: intelligence signals to detect phishing. Red boxes: stakeholders who get reports from threat intelligence organizations.

Methodology

- Receive 15,126 newly registered phishing domains between July 5, 2023 and May 23, 2024.
- Query multiple services to identify the domain registrar, hosting IP address, autonomous system (ASes), TLS certificate details.
- Perform passive DNS to find the first time and the last time the domains resolved to an IP address.
- Check the domains for Antivirus detection on VirusTotal and Google Safe-Browsing.

RQ1: What infrastructure do criminals abuse to host newly registered phishing domains?

AS Numbers	AS Names	Domains
AS200593	Prospero OOO	1 001
AS16509, AS14618	Amazon.com Inc	736
AS132203, AS45090	Tencent	421
AS45102	Alibaba (US) Technology Co.	351
AS47846	SEDO GmbH	321
AS54467, AS6134	XNNET LLC	238
AS133618	Trellian Pty. Limited	229
AS200019	ALEXHOST SRL	218
AS47583, AS204915	Hostinger International Limited	186
AS46606	Unified Layer	169

Table 7: Top 10 Autonomous Systems hosting newly registered phishing domains.

Prospero OOO identified as Bulletproof Hosting Provider (BPH)

https://www.intrinsec.com/wp-content/uploads/2024/11/TLP-CLEAR-PROSPERO-Proton66-Uncovering-the-links-between-bulletproof-networks.pdf

Prospero OOO's IP addresses hosts more phishing domains

IP Address	Our Dataset	Spamhaus pDNS	
	Domains	Domains	Hostnames
IP 1	327	2 644	2 980
IP 2	296	1 473	2 077
IP 3	121	696	886
IP 4	115	1 686	2 072

Table 8: Four IP Addresses from 'Prospero OOO' (AS200593) that host newly registered domains abused for phishing.

Prospero OOO involved in malicious activities till date!

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Notorious Malware, Spam Host “Prospero” Moves to Kaspersky Lab

February 28, 2025 27 Comments

One of the most notorious providers of abuse-friendly “bulletproof” web hosting for cybercriminals has started routing its operations through networks run by the Russian antivirus and security firm **Kaspersky Lab**, KrebsOnSecurity has learned.

Security experts say the Russia-based service provider **Prospero OOO** (the triple O is the Russian version of “LLC”) has long been a persistent source of malicious software, botnet controllers, and a torrent of phishing websites. Last year, the French security firm **Intrinsec** detailed Prospero’s connections to bulletproof services advertised on Russian cybercrime forums under the names **Securehost** and **BEARHOST**.

Search KrebsOnSecurity

SEARCH

Recent Posts

https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab/

RQ2: How long are these domains active?

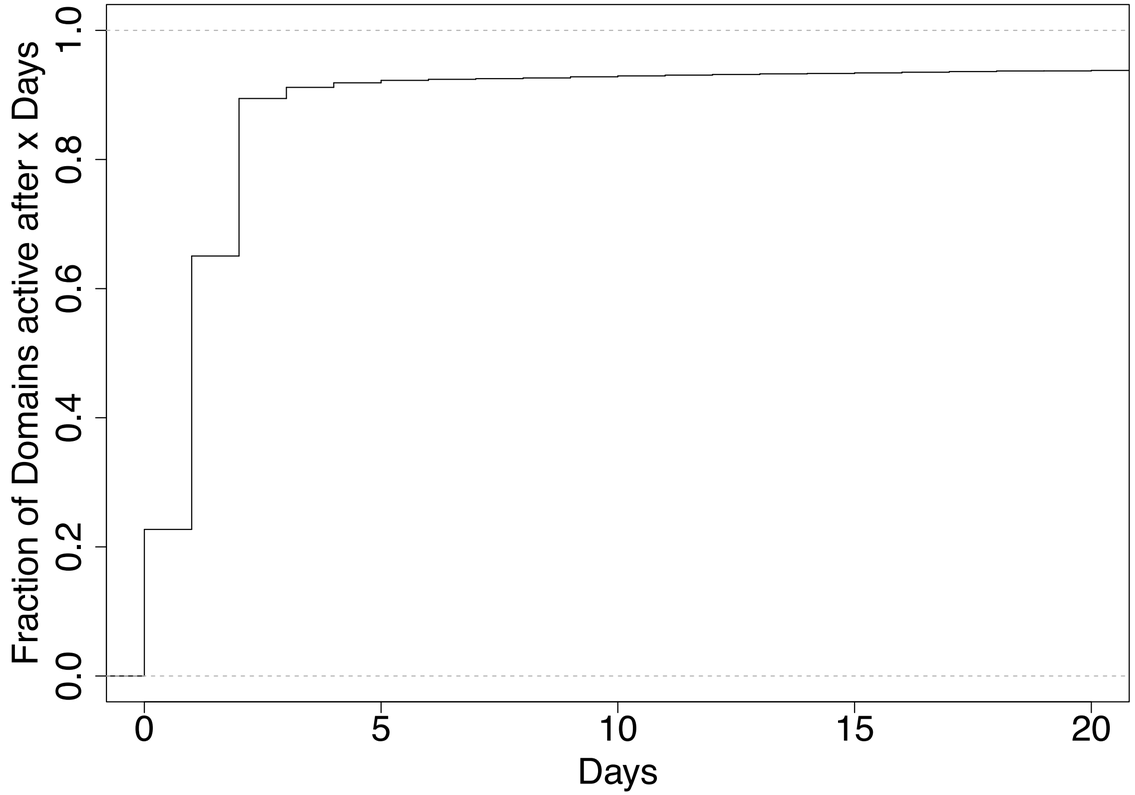
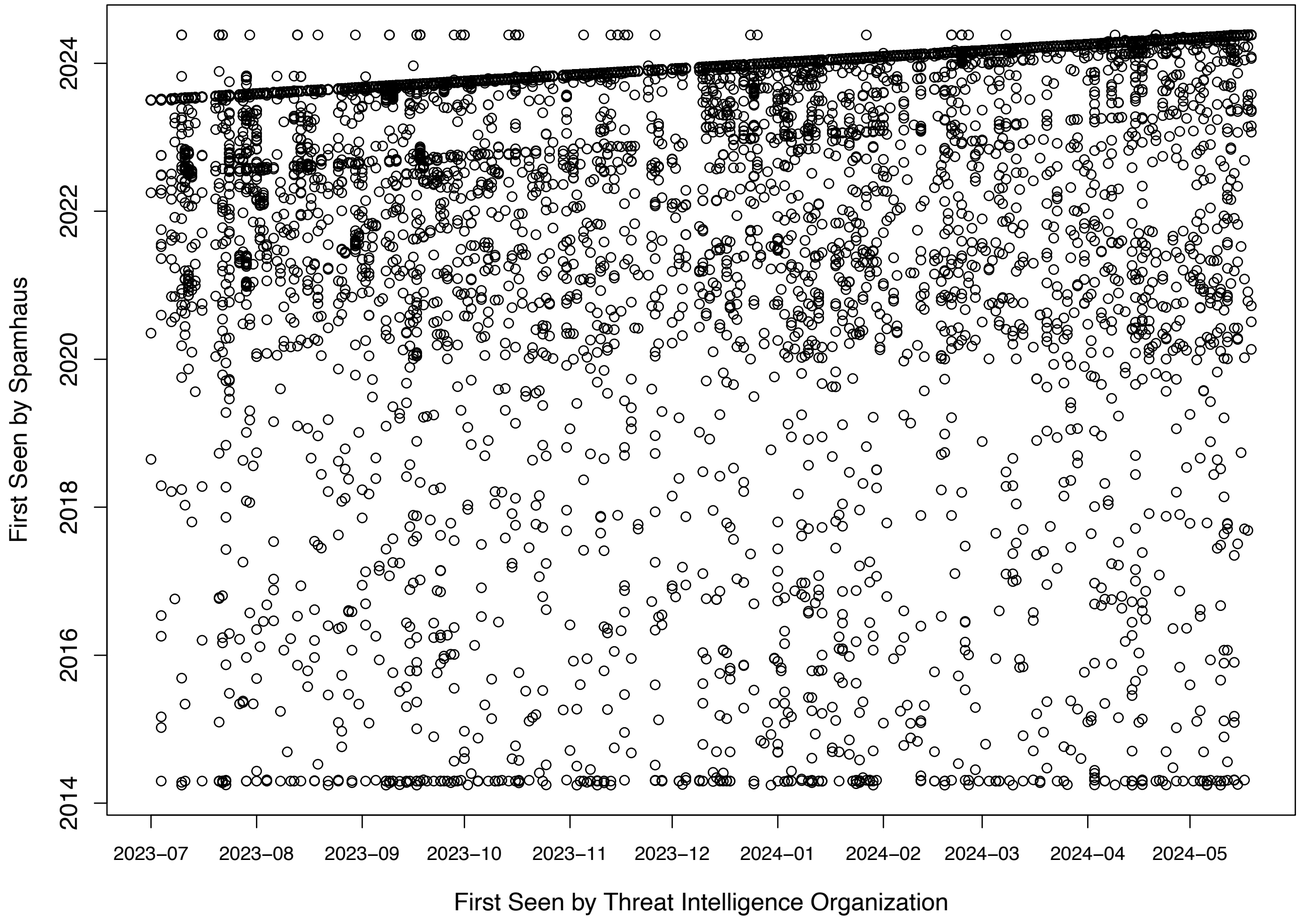


Figure 6: Cumulative distribution for the number of days newly registered phishing domains were active ($n = 14\,112$) with a median of 1 day and mean of 8.6 days.

Criminals re-register phishing domains



Conclusion

- Criminals register and re-register new domains to conduct (SMS) phishing.
- With the surge in smishing, the amount of newly registered phishing domains have also increased.
- The infrastructure criminals abuse keeps changing over time.
  - NameSilo - most abused domain registrar
  - ‘.com’ - the most abused TLD
  - We identify a new bulletproof hosting provider as the top AS.
- Stakeholders such as registrars do not consider prior domain abuse before providing services.

Checkout our paper:

Examining Newly Registered Phishing Domains at Scale

Sharad Agarwal*[1] and Marie Vasek†[1]

[1]Department of Computer Science, University College London (UCL)

sharad.agarwal@ucl.ac.uk

Abstract

Phishing has been prevalent for over two decades, evolving recently into new forms, such as smishing or SMS phishing. Despite its long reign, it continues to be significant, deceiving victims globally. Cybercriminals compromise benign websites or register new domains to host phishing web pages. These pages impersonate brands and lure victims into providing their personal or financial details. The infrastructure criminals exploit differs for compromised benign websites and newly registered domains, requiring different mitigation approaches. In this paper, we investigate new domains that cybercriminals register with the sole intent to host phishing websites. We analyze 15 126 unique newly registered domains over a period of 11 months. These domains have an average lifetime of 8.6 days, and miscreants re-register old domains to use them for phishing. The third-party infrastructure these domains exploit differs greatly from infrastructure where hacked websites or the general population of websites concentrate. This allows us insight into where efforts can be taken to take down these maliciously registered domains quicker, from a relatively new ASN to the `.COM` registry to more anonymous registrars. From our findings, we derive a set of recommendations for stakeholders towards reducing the effects of this scourge.

Full paper: http://kmlabcw.iis.u-tokyo.ac.jp/weis/2025/doc/proceedings/WEIS2025_paper_17.pdf

WEIS 2025

https://sharad1126.github.io/

CDA

Backup Slides

Compromised/Hacked phishing domains

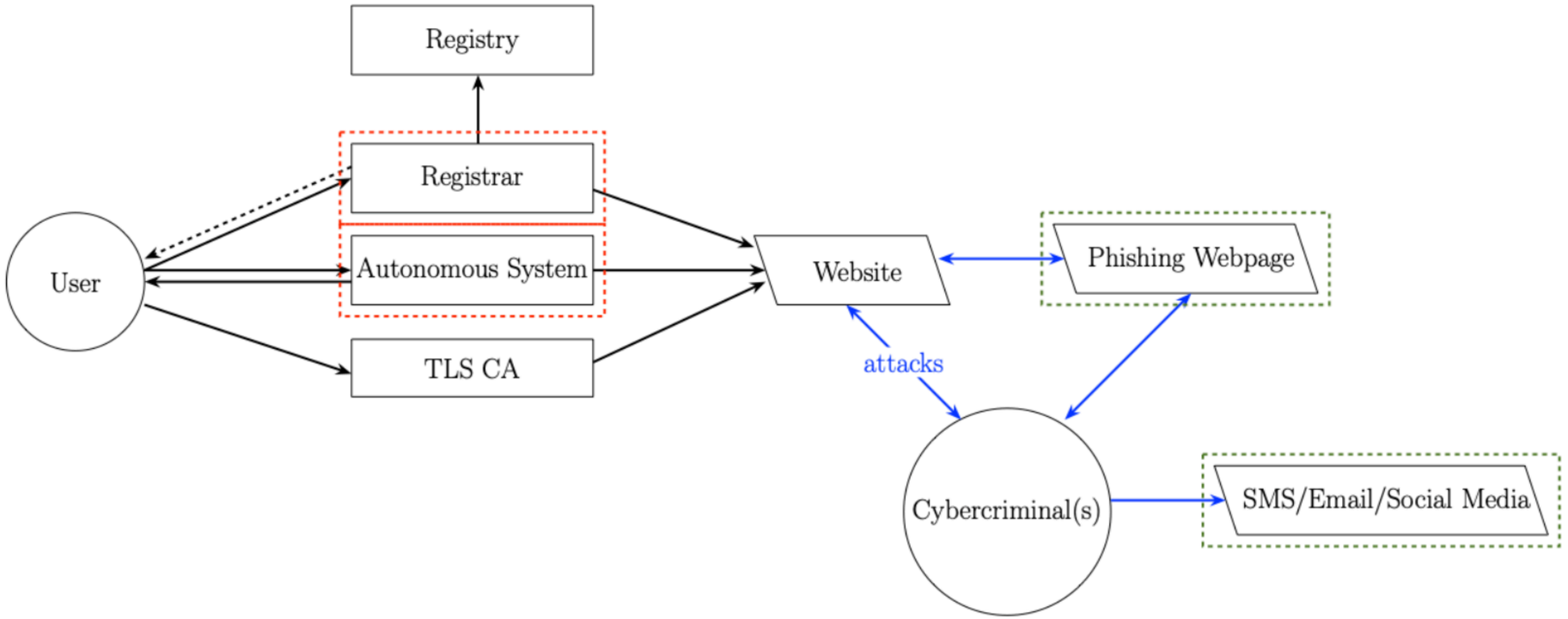


Figure 2: Cybercriminals host a phishing webpage by compromising a legitimate website. Black lines: user activities and stakeholder interactions. Blue lines: cybercriminal activities. Green boxes: intelligence signals to detect phishing. Red boxes: stakeholders who get reports from threat intelligence organizations.

RQ2: What brands do cybercriminals impersonate?

Brands	Sector	Domains
Royal Bank of Canada	Financial Institution/Banking	1 268
Royal Mail	Delivery/Shipping	1 015
Santander	Financial Institution/Banking	916
DHL	Delivery/Shipping	889
Apple	Tech	775
EVRI	Delivery/Shipping	702
An Post	Delivery/Shipping	497
Barclays	Financial Institution/Banking	277
Deutsche Bank	Financial Institution/Banking	240
AIB	Financial Institution/Banking	229

Table 10: Top 10 brands impersonated to lure victims.

Criminals wait to conduct phishing after registering domains