On SMS Phishing Tactics and Infrastructure

*Aleksandr Nahapetyan[†], **Sathvik Prasad**[†], Kevin Childs[†], Adam Oest[‡], Yeganeh Ladwig[‡], Alexandros Kapravelos[†], **Bradley Reaves**[†]*

[†]North Carolina State University, [‡]PayPal Inc.

NC STATE UNIVERSITY

PayPal

What will you learn from this talk?

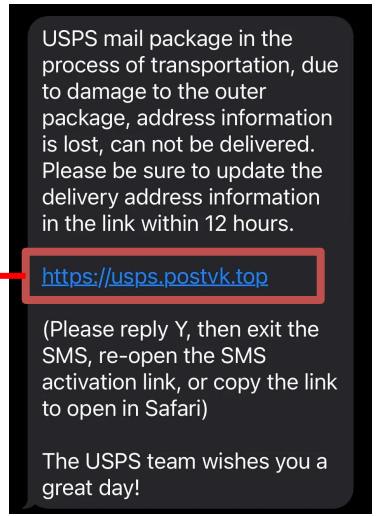
How to collect your own data on SMS abuse

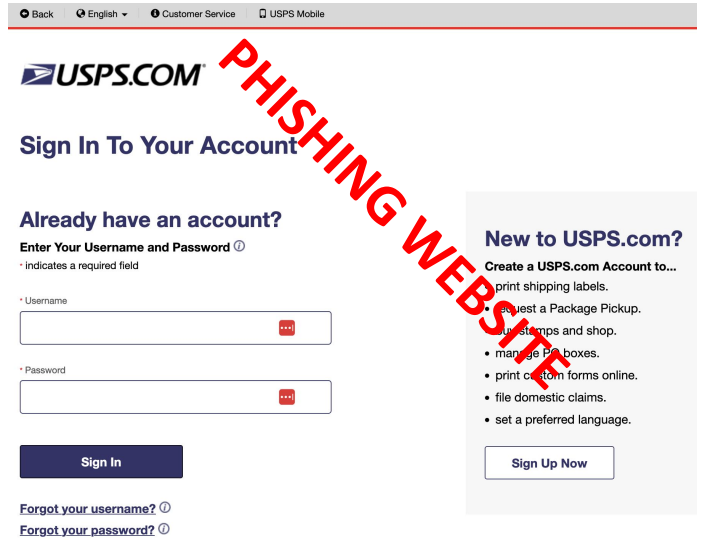
How to go from millions of SMS messages to identify phishing campaigns and operations

Current tactics and procedures used by SMS phishing operations

Classic SMS Phishing - USPS Package Delivery

Phishing URL

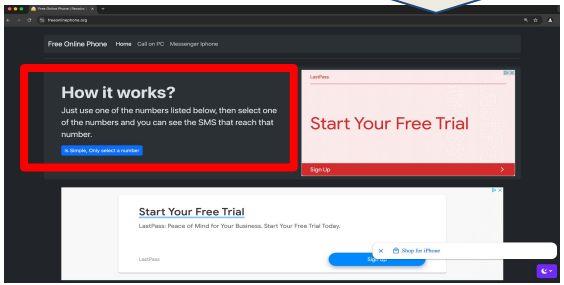




Where can you find public SMS data?

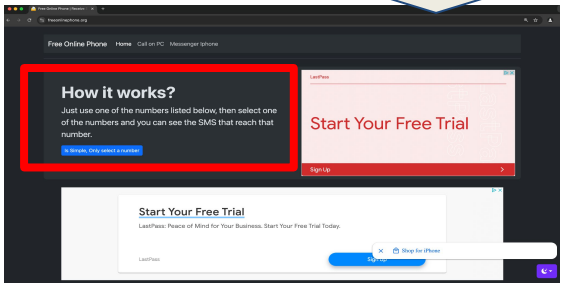
Public Disposable-Number SMS “Gateways”

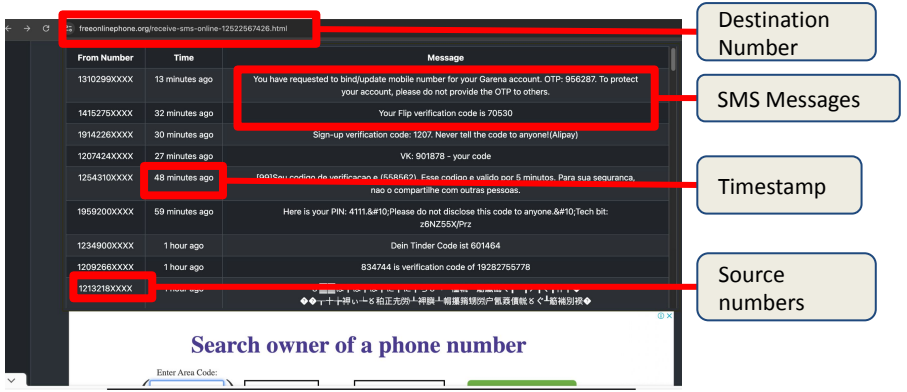
“Just use one of the numbers listed below,
then select one of the numbers,
and you can see the SMS that reach that number”



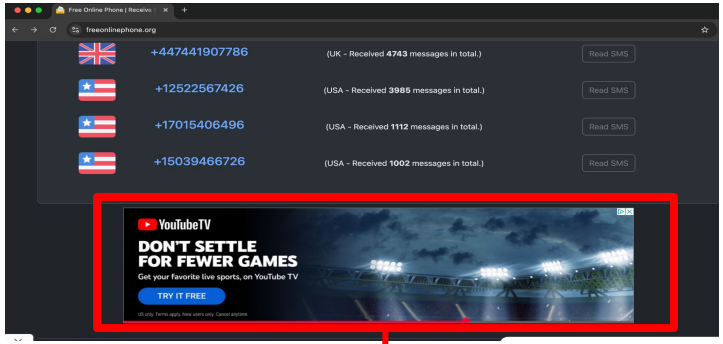
Public Disposable-Number SMS “Gateways”

“Just use one of the numbers listed below,
then select one of the numbers,
and you can see the SMS that reach that number”





Why do such websites (SMS gateways) exist?



Advertisements

Free phone numbers that can receive SMS and show the text on the website

Website owner serves ads to generate $$ when people visit the webpage

Why do people use these SMS gateways?

Phone number verification to create online accounts

Why do people use these SMS gateways?

Phone number verification to create online accounts

Generate One Time Passwords (OTPs) or One Time Codes

Why do people use these SMS gateways?

Phone number verification to create online accounts

Generate One Time Passwords (OTPs) or One Time Codes

Bypass geographic restrictions (create online accounts in the US without owning a North American phone number)

Why do people use these SMS gateways?

Phone number verification to create online accounts

Generate One Time Passwords (OTPs) or One Time Codes

Bypass geographic restrictions (create online accounts in the US without owning a North American phone number)

To test SMS phishing campaigns!

SMS Analysis vs. Web Analysis

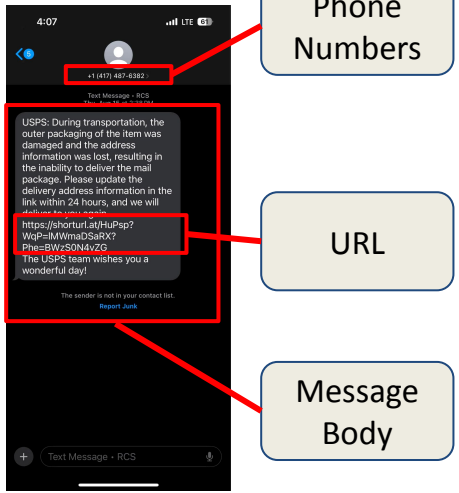
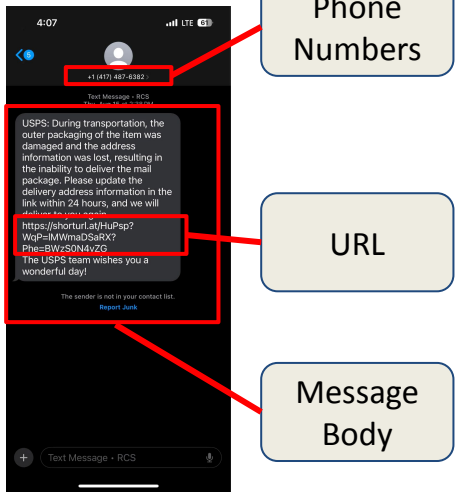


Image Source: https://www.reddit.com/r/scambait/comments/1eznw12/im_assuming_this_is_a_scam_right/

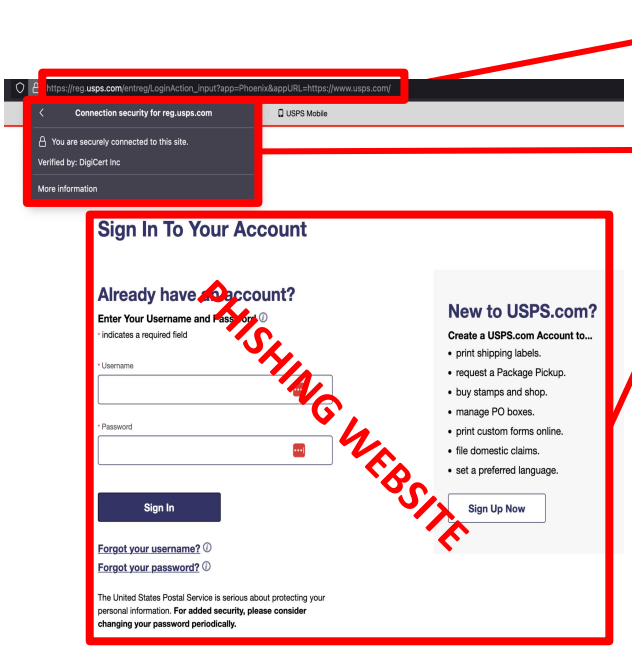
SMS Analysis vs. Web Analysis



Phone Numbers

URL

Message Body



Domain and URL

TLS Certificate

Webpage source code

Image Source: https://www.reddit.com/r/scambait/comments/1eznw12/im_assuming_this_is_a_scam_right/

Phishing websites contain invaluable clues!

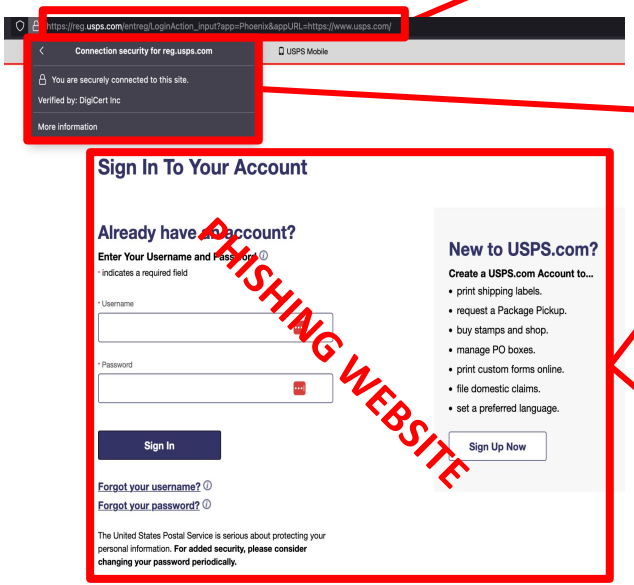
Domain and URL
Domain and subdomain details
Domain age and history
Domain reputation
Domain registrar
Domain ownership
Hosting provider

TLS Certificate
Certificate issuer
Issue date
Start date and expiration date

Webpage source code
HTML, JavaScript, CSS…

Website behaviors
Cloaking (evading detection)
Fingerprinting visitor browsers

..and much more

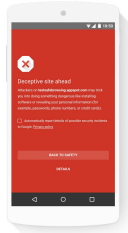


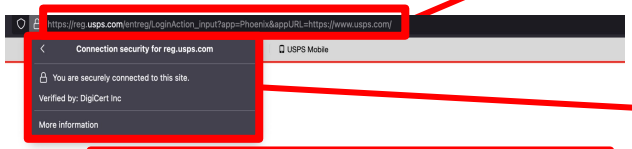
Defenders have an advantage on the Web!

Domain and URL
Domain and subdomain details
Domain age and history
Domain reputation
Domain registrar
Domain ownership
Hosting provider

VIRUSTOTAL

APWG

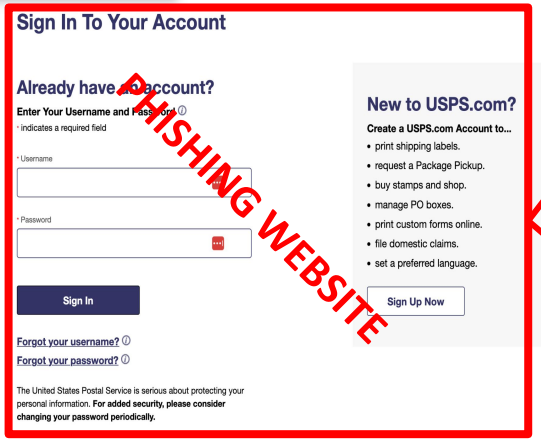




TLS Certificate
Certificate issuer
Issue date
Start date and expiration date

Certificate Transparency

ICANN Lookup (WHOIS)

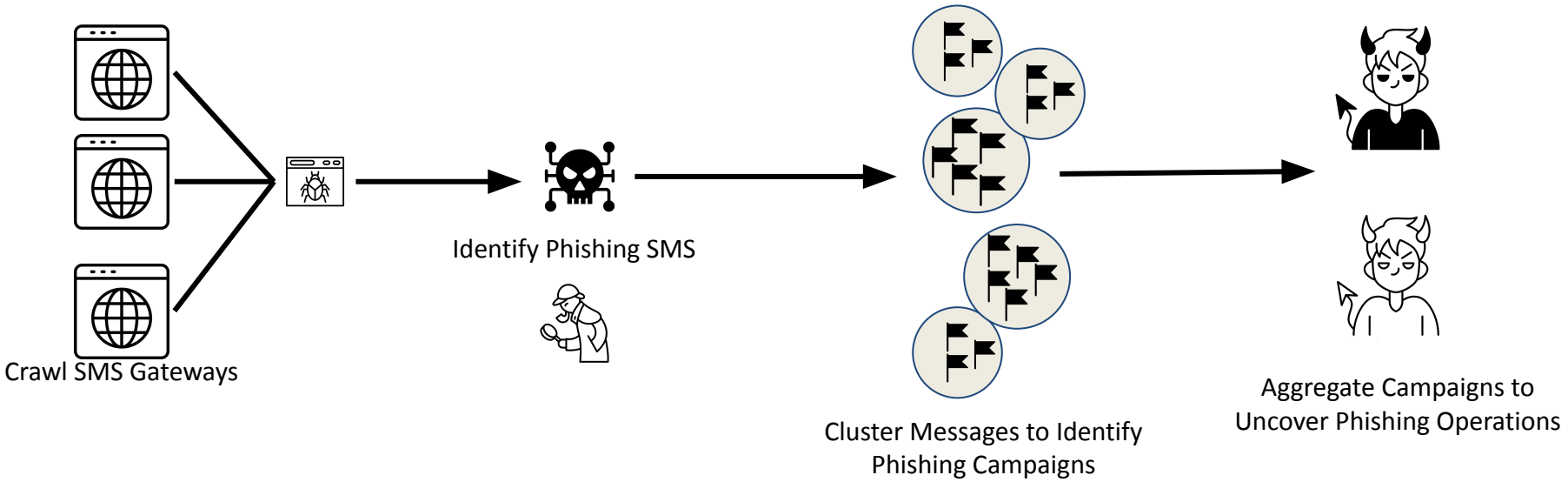


Webpage source code
HTML, JavaScript, CSS…

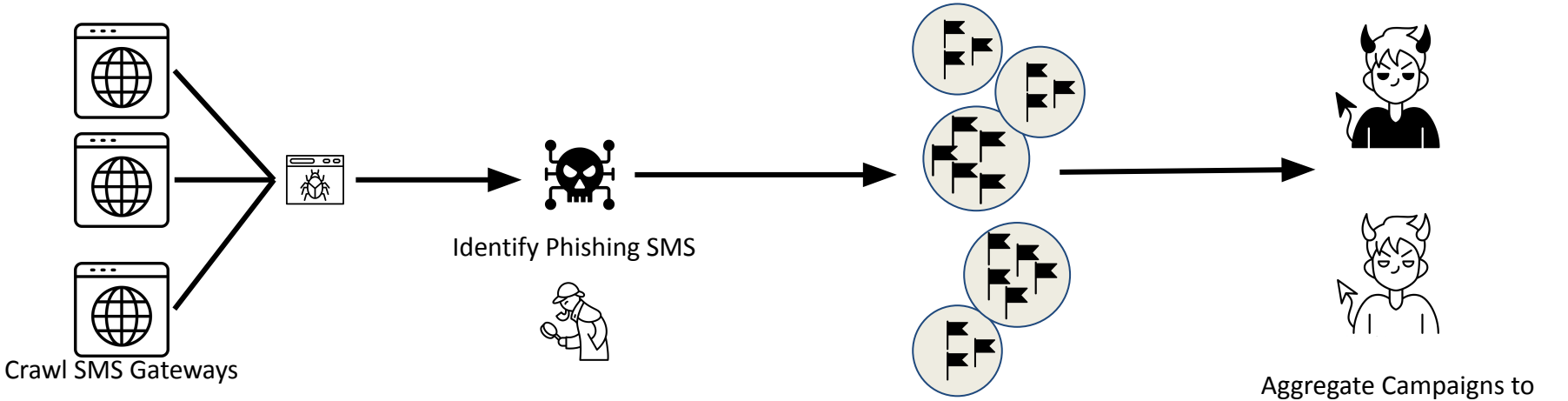
Website behaviors
Cloaking (evading detection)
Fingerprinting visitor browsers

..and much more

Uncovering Phishing Operations from SMS Gateways

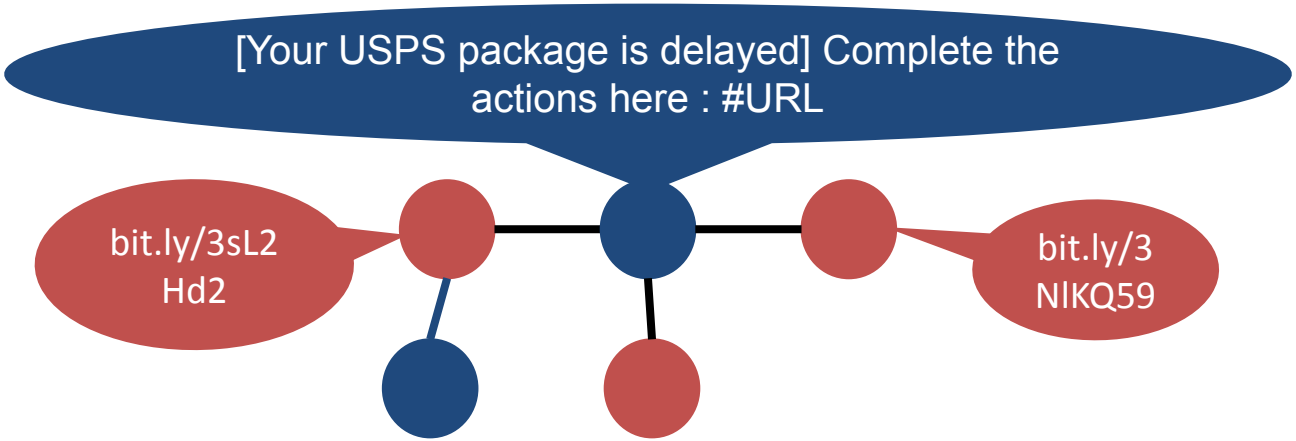


Uncovering Phishing Operations from SMS Gateways



More than 35k phishing campaigns and over 600 phishing operations

From Campaigns to Operations



SMS with a URL (message)

Domain or URL (infrastructure)

Dramatic increase in abuse data on SMS Gateways

View from 2015		*View from 2023*
8 gateways, over 1.5 years of crawling	→	11 gateways, about 2 years of crawling
380k messages	→	200 Million messages
Only a handful of phishing SMS	→	Average of 170 phishing SMS messages **daily**
About 25 phishing websites	→	Around 2,800 unique phishing websites

2016 Study: "Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways"
2023 Study: "On SMS Phishing Tactics and Infrastructure"

Why do we see phishing on public SMS gateways?

SMS Gateways as Testing Grounds for Phishers

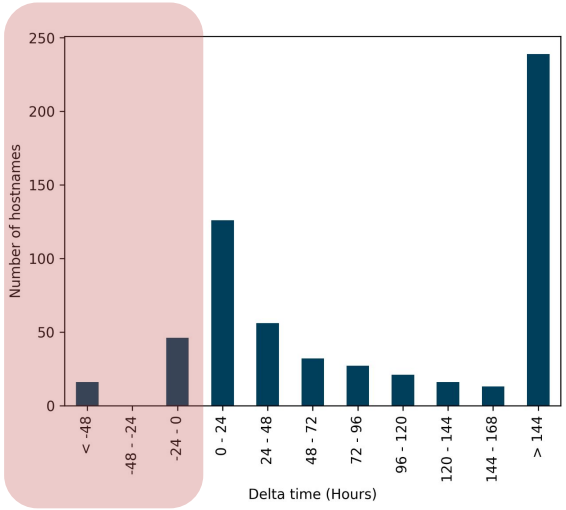
We found 45 operations (161 campaigns) that were testing various SMS delivery routes by changing the SMS body

`SMS Body #URL` **`route:[0-9]`**

An unusual login attempt was made on 04/06 at 16:42\nIf this was NOT you, please visit:#URL	**route:6**
An unusual login attempt was made on 06/06 at 7:42\nIf this was NOT you, please visit:#URL	**route:6**
An unusual login attempt was made on 04/06 at 16:42\nIf this was NOT you, please visit:#URL	**route:2**
An unusual login attempt was made on 04/06 at 16:42\nIf this was NOT you, please visit:#URL	**route:3**

Operations test campaigns before they generate web certificates!

We compared the timestamps of the earliest phishing message in a campaign with the issue times of TLS certificates

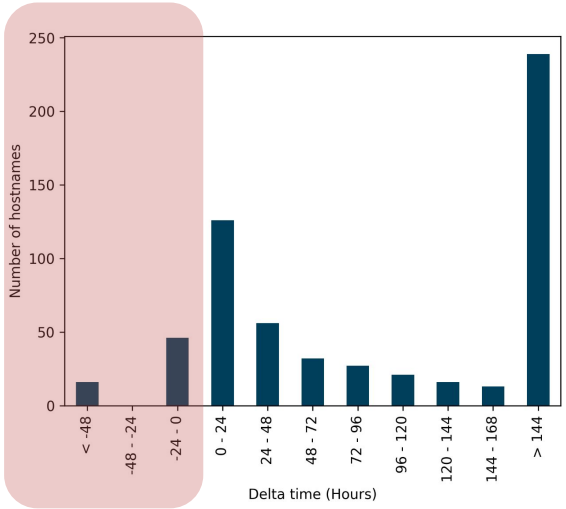


Operations test campaigns before they generate web certificates!

We compared the timestamps of the earliest phishing message in a campaign with the issue times of TLS certificates

We uncovered 16 campaigns that sent out test phishing messages to SMS gateways before they generated their TLS certificates

Takeaway: By monitoring gateways, we can see phishing **before the victims!**



What Infrastructure do these Operations Use?

Hiding behind redirection: Over 70% of phishing URLs redirect to a different host name

Hiding behind URL shorteners: Over 600 URLs were shortened using public and private URL shortening services

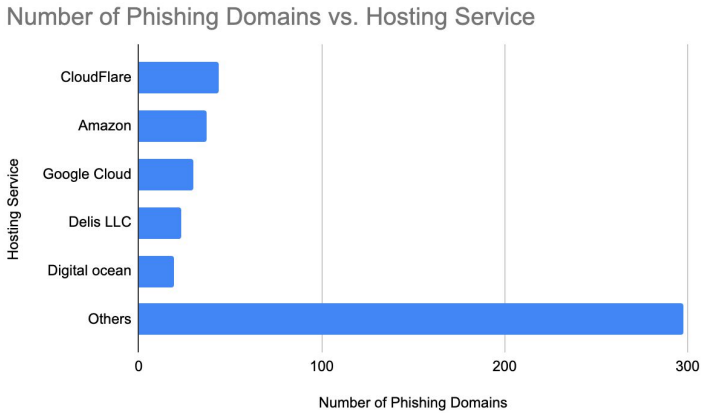
Second-Level Domain	Number of URLs	Public shortener?
tx[.]vc	**263**	**No**
shrtlink[.]net	**173**	**No**
qi[.]lv	83	Yes
shor[.]td	70	Yes
kvo6[.]io	**50**	**No**

Caution: These domains may be malicious.

Where are these phishing web pages hosted?

Most phishing websites we uncovered were hosted on **well-known public cloud providers**

Cloudflare, AWS and GCP were the most popular options, along with a long tail of other providers



Brand Impersonation and Phishing

We extracted *named entities* (organization names, product names, etc.)

Brand Impersonation and Phishing

We extracted *named entities* (organization names, product names, etc.)

The top entities mentioned were Apple, CommBank, DHL, and the Australian government, but…

87% of operations didn't mention detectable named entities

But wait, there's more! (in the paper)

List of SMS Gateways

Deep dive into phishing kits – tools that phishers use to easily create phishing websites

Analysis of online forums and platforms where illicit bulk SMS delivery services advertise

..and many other interesting details

Robocall Science

On our public outreach website you will find:

- PDFs of all our published work
- Links to our code and dataset releases
- A handy newsletter to be informed when we put something out
- How to work with us

https://robocall.science

Key Takeaways

Public SMS gateways are a great resource to gather threat intelligence about phishing campaigns.

Our techniques demonstrate how you can process millions of SMS messages and reliably uncover phishing operations.

We highlight how phishing operations use SMS gateways to test their campaign, employ deception to hide behind URL shorteners and impersonate well-known brands to trick victims.

Contact

Sathvik Prasad: snprasad@ncsu.edu
Brad Reaves: bgreaves@ncsu.edu

Robocall Science

https://robocall.science