Patterns in malicious campaigns

CPS May 2026

Rowena Schoo, Senior Director, Industry Affairs & Policy, NetBeacon Institute

Today

1. About
2. Case study: Winter Fuel malicious phishing campaign
3. What is ‘subdomain cloaking’?
4. Why care?
5. Implications for operators
6. Q&A

NetBeacon Institute

Vision: A Safer Internet for Everyone

- Created and operated by Public Interest Registry (.ORG) in service of its nonprofit mission since 2021.
- Non-commercial, all our products and services are free.
- Education, Innovation and Collaboration.

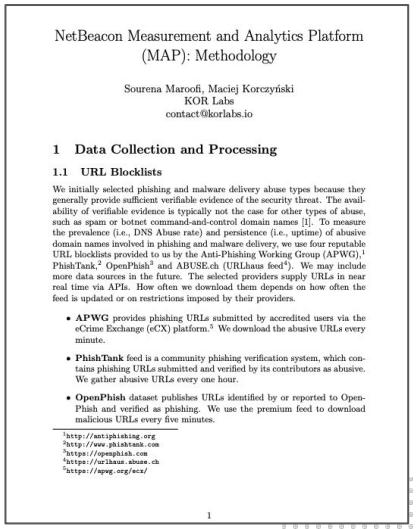
NetBeacon MAP

Measures the prevalence & persistence of phishing and malware in the DNS.

Principles:

- Transparency
- Credibility and independence
- Accuracy and reliability

Delivery partner: KOR Labs, Grenoble Alpes University



NetBeacon Measurement and Analytics Platform (MAP): Methodology

Sourena Maroofi, Maciej Korczyński
KOR Labs
contact@korlabs.io

1 Data Collection and Processing

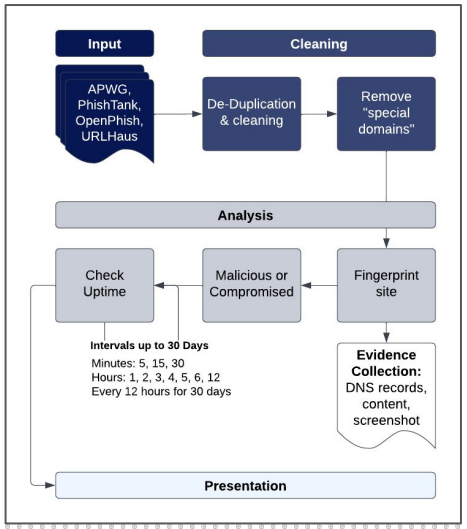
1.1 URL Blocklists

We initially selected phishing and malware delivery abuse types because they generally provide sufficient verifiable evidence of the security threat. The availability of verifiable evidence is typically not the case for other types of abuse, such as spam or botnet command-and-control domain names [1]. To measure the prevalence (i.e., DNS Abuse rate) and persistence (i.e., uptime) of abusive domain names involved in phishing and malware delivery, we use four reputable URL blocklists provided to us by the Anti-Phishing Working Group (APWG),[1] PhishTank,[2] OpenPhish[3] and ABUSE.ch (URLhaus feed[4]). We may include more data sources in the future. The selected providers supply URLs in near real time via APIs. How often we download them depends on how often the feed is updated or on restrictions imposed by their providers.

- **APWG** provides phishing URLs submitted by accredited users via the eCrime Exchange (eCX) platform.[5] We download the abusive URLs every minute.
- **PhishTank** feed is a community phishing verification system, which contains phishing URLs submitted and verified by its contributors as abusive. We gather abusive URLs every one hour.
- **OpenPhish** dataset publishes URLs identified by or reported to OpenPhish and verified as phishing. We use the premium feed to download malicious URLs every five minutes.

[1] http://antiphishing.org
[2] http://www.phishtank.com
[3] https://openphish.com
[4] https://urlhaus.abuse.ch
[5] https://apwg.org/ecx/

1



https://netbeacon.org/map-analytics/

NetBeacon Reporter™

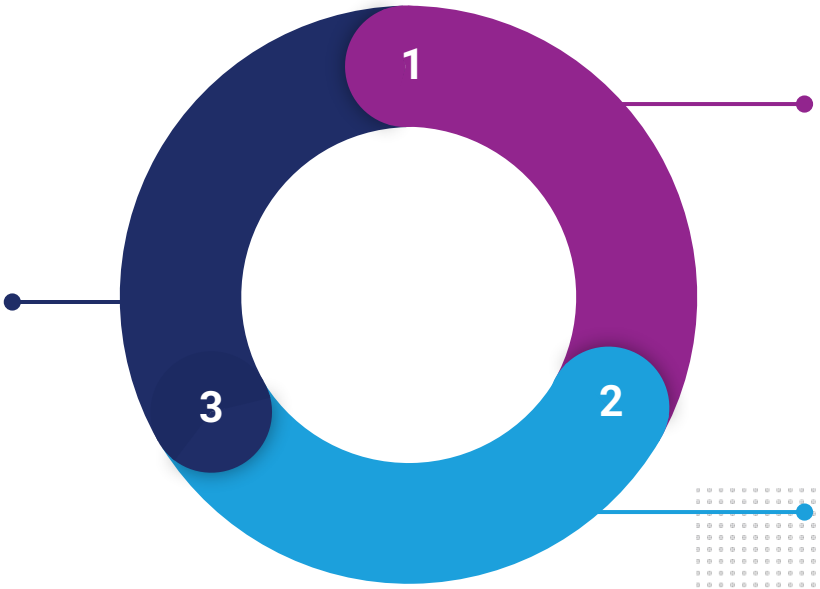
- Our centralized DNS Abuse reporting conduit to simplify and improve abuse reporting
- Provides a single, simple interface for abuse reporters
- Provides consistent, evidenced, actionable abuse reports
- Automatically distributes
- Monitors mitigation
- Delivery Partner: CleanDNS

Malicious phishing & malware

Investigate

High abuse rates, unusual patterns and spikes.

Retrospective 🔍



Disrupt

NetBeacon MAP → NetBeacon Reporter when still live and well evidenced.

Real time 🏃‍♀️

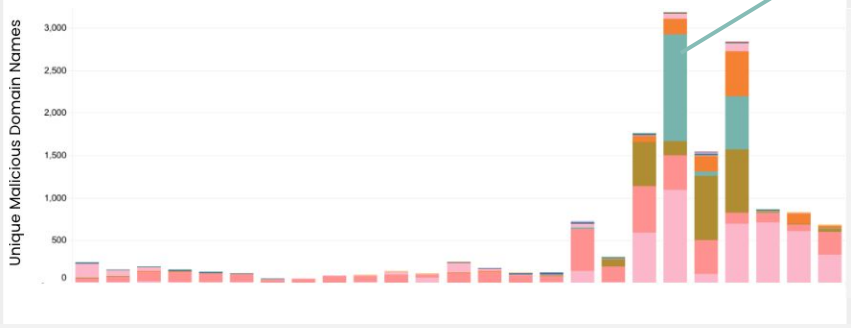
Understand

Public analysis and individualized dashboards in NetBeacon MAP.

~2 months delay ⏳

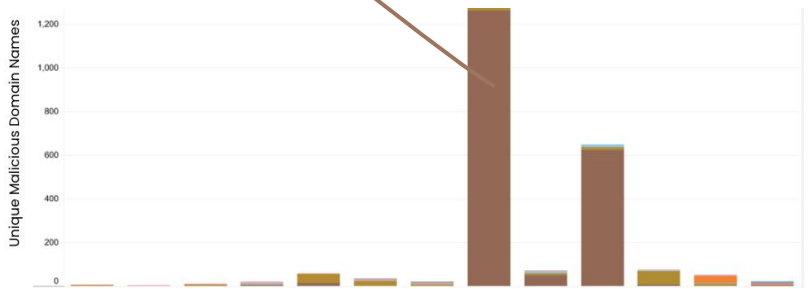
August 2025

Aceville



Jan 2024 Jan 2026

.qpon



Jan 2025 Jan 2026

Investigation

- Underlying domains
- Noticed large batches starting with ‘uk-’
- Queried wider NetBeacon MAP data
- Removed 26 unrelated, left with >2000 unique domain names

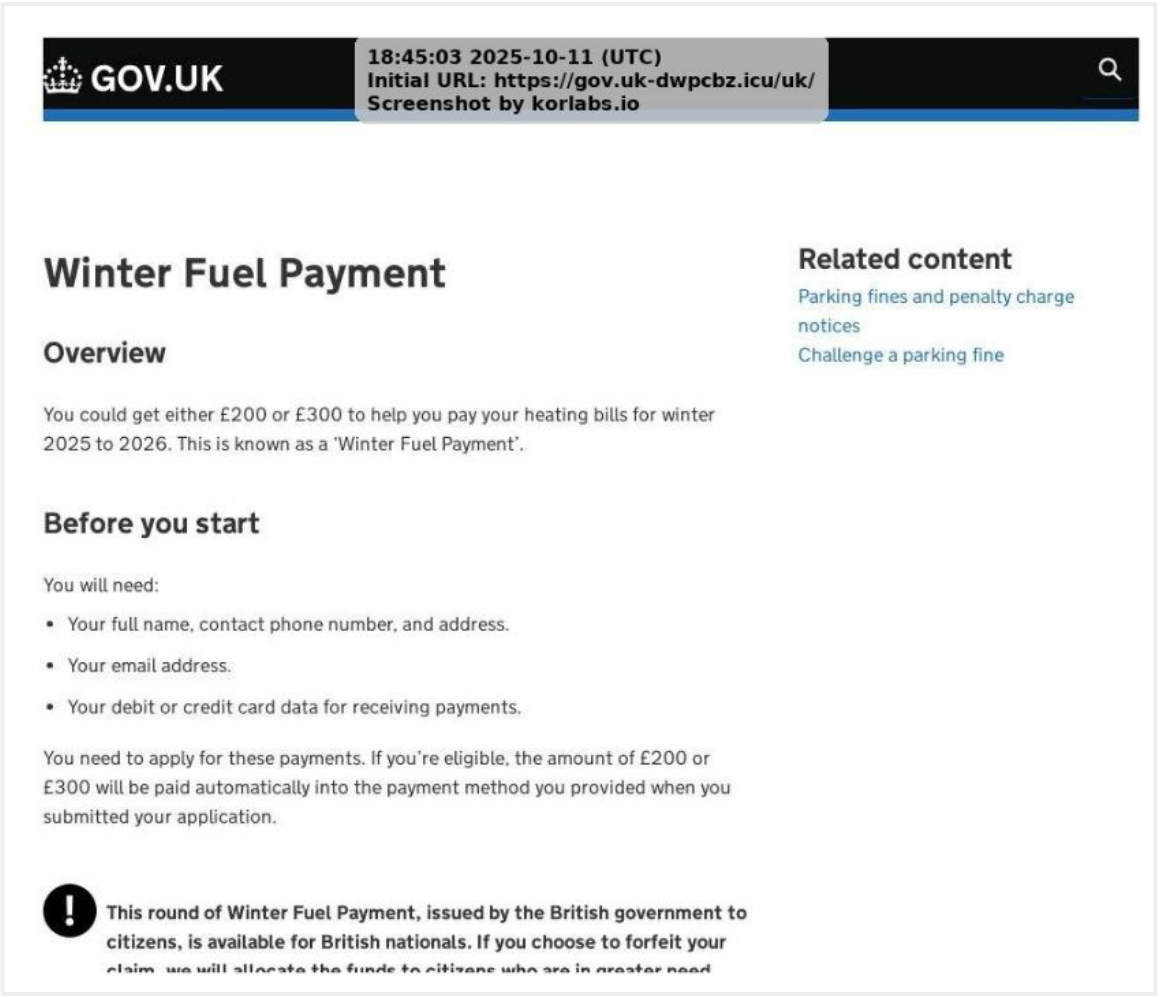
Categories

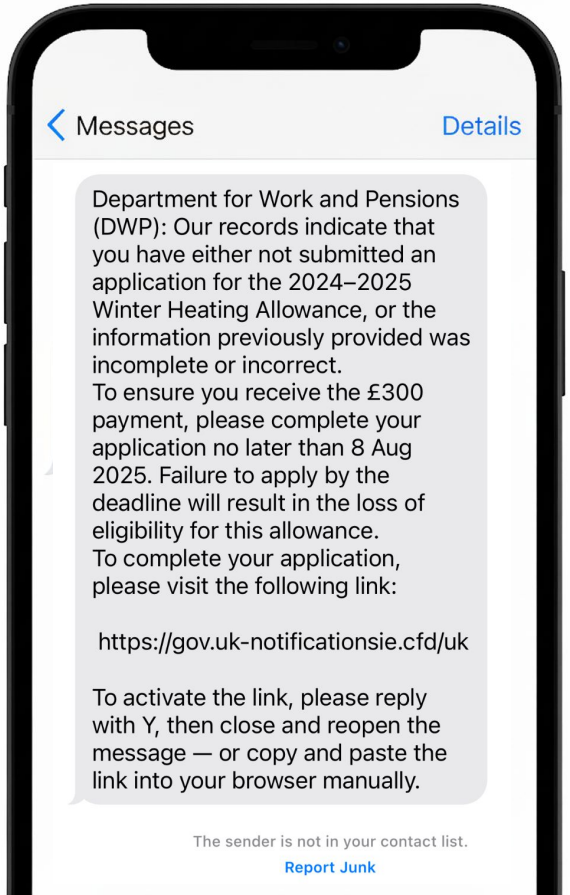
uk-dwpukd.cfd
uk-dwpuke.cfd
uk-dwpukh.cfd
uk-dwpuki.cfd
uk-dwpukl.cfd
uk-dwpukm.cfd
uk-dwpukn.cfd
uk-dwpukp.cfd
uk-dwpukr.cfd
uk-dwpuks.cfd
uk-dwpukt.cfd
uk-dwpuku.cfd
uk-dwpukv.cfd
uk-dwpukw.cfd
uk-dwpukx.cfd

uk-reminderae.cfd
uk-reminderae.icu
uk-reminderag.bond
uk-reminderag.cfd
uk-reminderag.icu
uk-reminderai.bond
uk-reminderai.cfd
uk-reminderai.icu
uk-reminderal.bond
uk-reminderal.cfd
uk-reminderal.icu
uk-reminderam.cfd
uk-reminderan.bond
uk-reminderan.cfd
uk-reminderan.icu

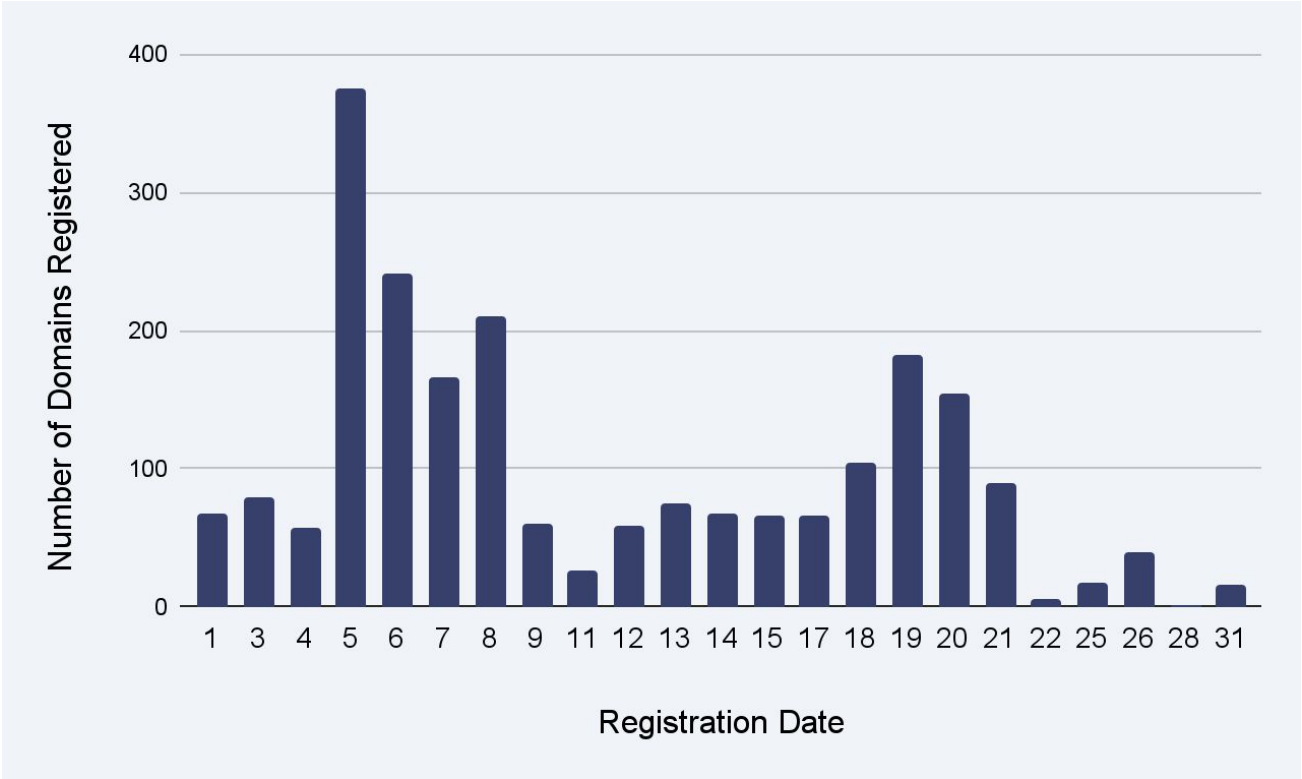
uk-winteav.bond
uk-winteaw.bond
uk-winteax.bond
uk-wintecs.bond
uk-wintecw.bond
uk-winteeb.qpon
uk-winteec.qpon
uk-winteev.bond
uk-winteex.bond
uk-winteez.bond
uk-winteha.qpon
uk-wintehc.bond
uk-wintehd.qpon
uk-wintehe.qpon
uk-wintehg.qpon
uk-wintehp.qpon

- **Winter/Fuel/Payment:** "winter" or "fuel"
- **DWP:** Contains the "dwp" acronym, which was prioritized above all other keywords
- **Subsidy/Grant:** "subsidy" or "grant"
- **Other:** call-to-action words like "**notification**" or "**claim**"

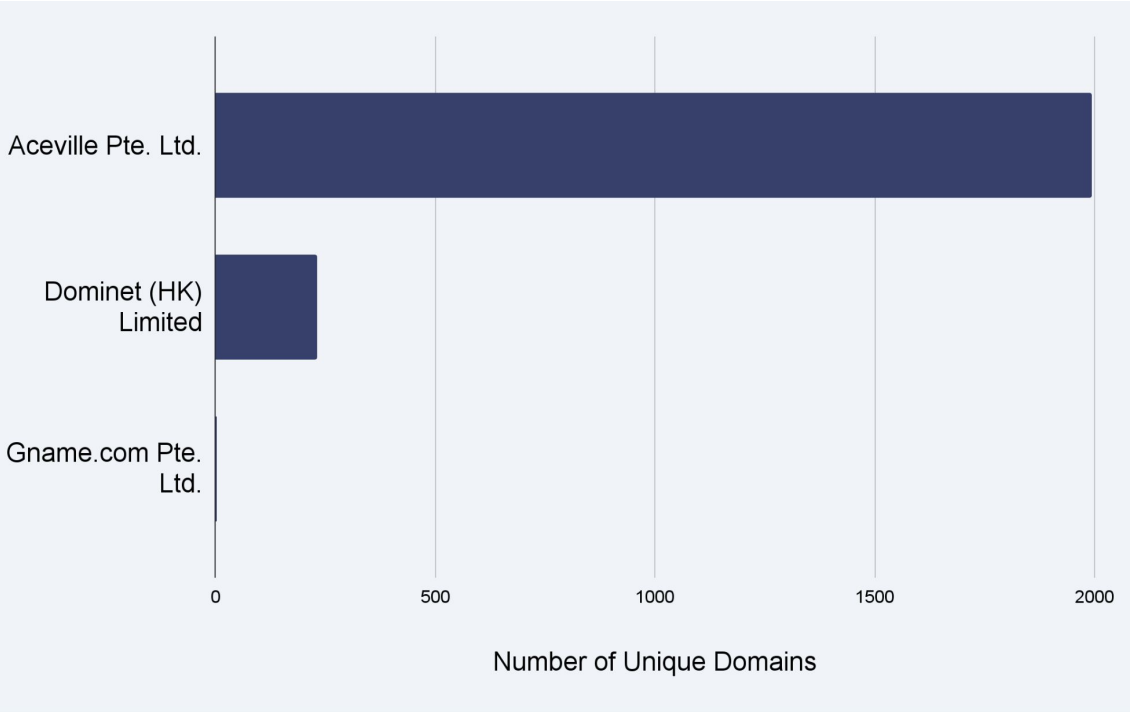

GOV.UK
18:45:03 2025-10-11 (UTC)
Initial URL: https://gov.uk-dwpcbz.icu/uk/
Screenshot by korlabs.io
Winter Fuel Payment
Overview
You could get either £200 or £300 to help you pay your heating bills for winter 2025 to 2026. This is known as a 'Winter Fuel Payment'.
Before you start
You will need:
Your full name, contact phone number, and address.
Your email address.
Your debit or credit card data for receiving payments.
You need to apply for these payments. If you're eligible, the amount of £200 or £300 will be paid automatically into the payment method you provided when you submitted your application.
This round of Winter Fuel Payment, issued by the British government to citizens, is available for British nationals. If you choose to forfeit your
Related content
Parking fines and penalty charge notices
Challenge a parking fine


Messages
Details
Department for Work and Pensions (DWP): Our records indicate that you have either not submitted an application for the 2024–2025 Winter Heating Allowance, or the information previously provided was incomplete or incorrect.
To ensure you receive the £300 payment, please complete your application no later than 8 Aug 2025. Failure to apply by the deadline will result in the loss of eligibility for this allowance.
To complete your application, please visit the following link:
https://gov.uk-notificationsie.cfd/uk
To activate the link, please reply with Y, then close and reopen the message — or copy and paste the link into your browser manually.
The sender is not in your contact list.
Report Junk

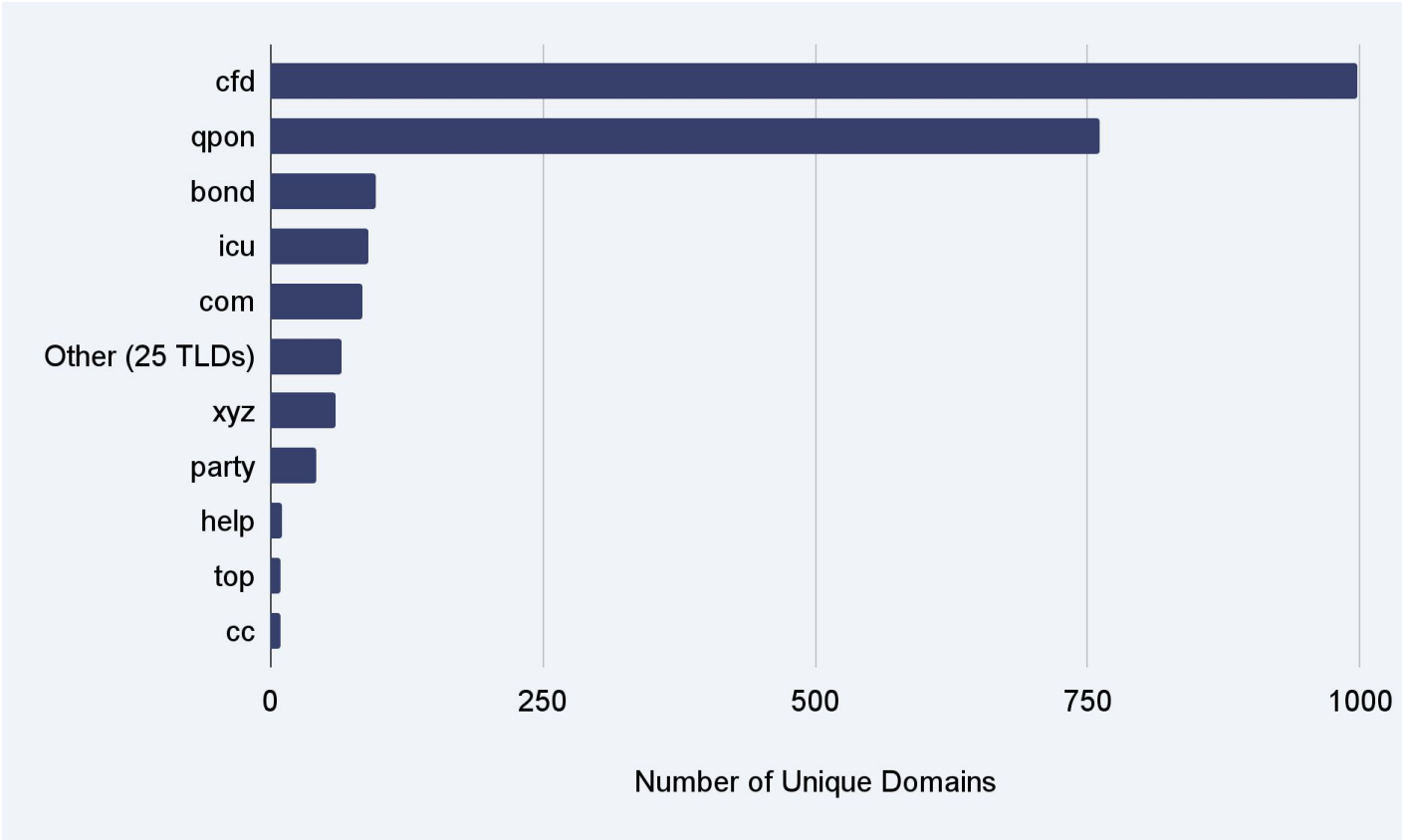
Timeline: August 2025



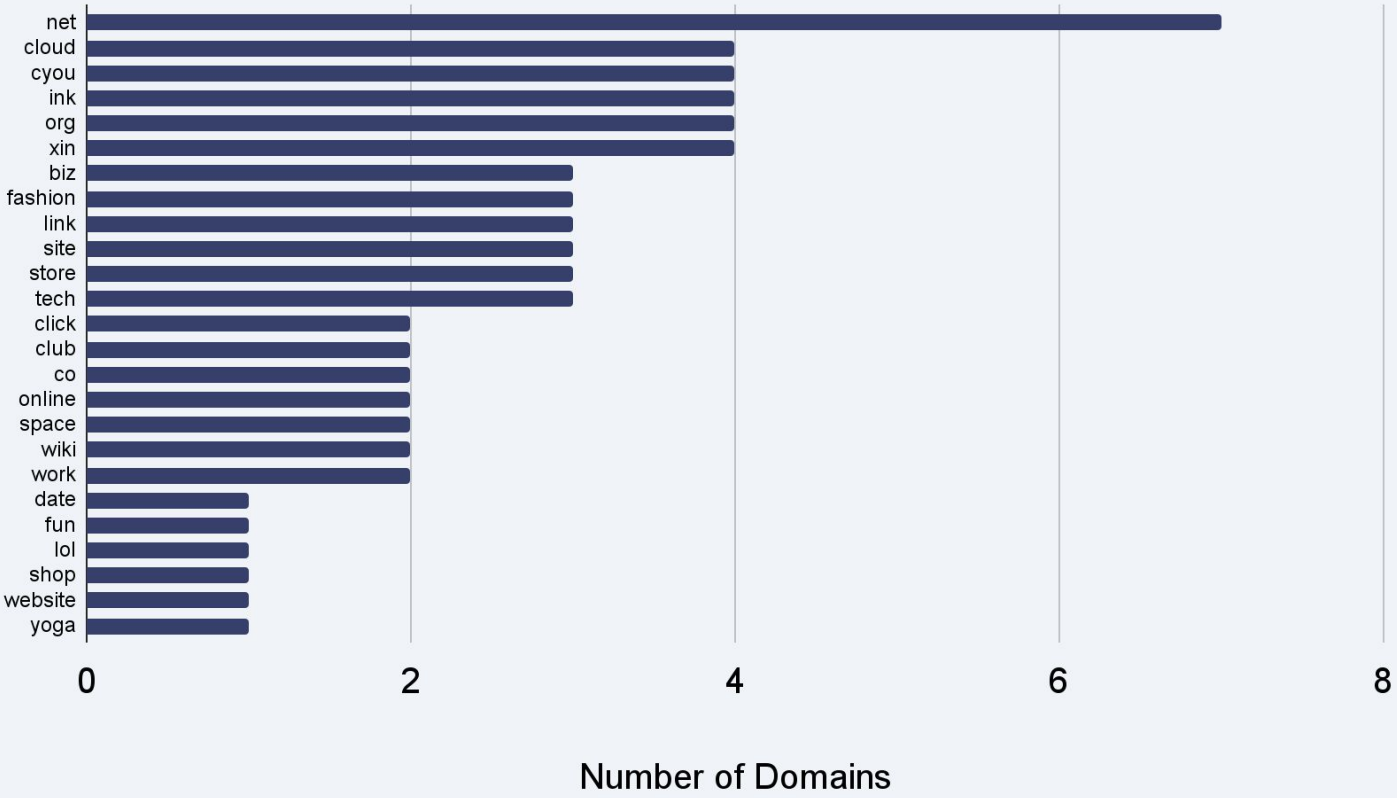
Registrar Credentials



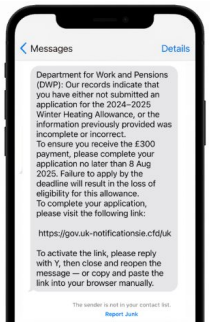
TLDs: “Top 10”


cfd
qpon
bond
icu
com
Other (25 TLDs)
xyz
party
help
top
cc
0
250
500
750
1000
Number of Unique Domains

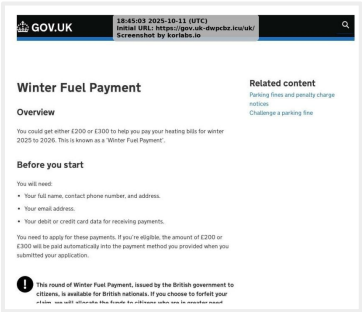
TLDs: “Other 25”



Evidenced Reports: Subdomains



https://gov.uk-notificationsie.cfd/uk



https://gov.uk-dwpcbz.icu/uk/

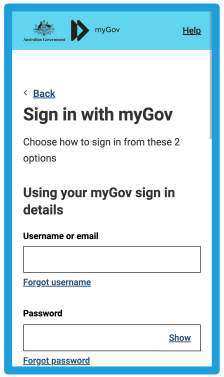
subdomain.domain.TLD

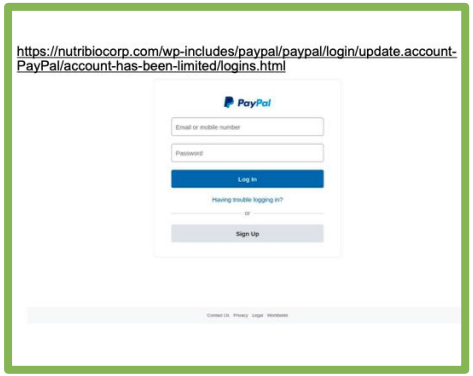
gov.uk-[keyword][random letters].[TLD]

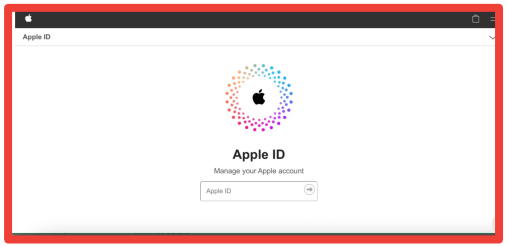
https://gov.uk-winterivx.qpon/uk
https://gov.uk-winterixo.qpon/uk
https://gov.uk-winteruhm.qpon/uk
https://gov.uk-winteruif.qpon/uk
https://gov.uk-winteruii.qpon/uk
https://gov.uk-winteruik.qpon/uk
https://gov.uk-winteruio.qpon/uk
https://gov.uk-winteruiu.qpon/uk
https://gov.uk-winterulz.qpon/uk
https://gov.uk-winteruoq.qpon/uk
https://gov.uk-winteruor.qpon/uk
https://gov.uk-winteruti.qpon/uk
https://gov.uk-winterutp.qpon/uk

Flavours of phishing

- **Malicious**: registered for the purpose of phishing auth-log-in-mygov[.]org
- **Compromised**: Typically via a website vulnerability localbakery[.]com/paypal/login/account-has-been-limited.html
- **Subdomain Service Abuse**: A legitimate service provider, which has a malicious user. http://ljwqmhbwvq.duckdns[.]org/en/
- **Subdomain Cloaking**: Malicious domain masquerading as subdomain service abuse https://gov.uk-dwpcbz.icu/uk/







https://gov.uk-winterivx.qpon/uk
https://gov.uk-winterixo.qpon/uk
https://gov.uk-winteruhm.qpon/uk
https://gov.uk-winteruif.qpon/uk
https://gov.uk-winteruii.qpon/uk
https://gov.uk-winteruik.qpon/uk
https://gov.uk-winteruio.qpon/uk
https://gov.uk-winteruiu.qpon/uk
https://gov.uk-winterulz.qpon/uk
https://gov.uk-winteruoq.qpon/uk
https://gov.uk-winteruor.qpon/uk
https://gov.uk-winteruti.qpon/uk
https://gov.uk-winterutp.qpon/uk

Subdomain Cloaking

Malicious domain masquerading as subdomain service abuse to evade detection.

Typically uses a subdomain to more effectively impersonate a trusted domain.

Often includes TLDs (e.g. gov-uk- de-).

Why care?

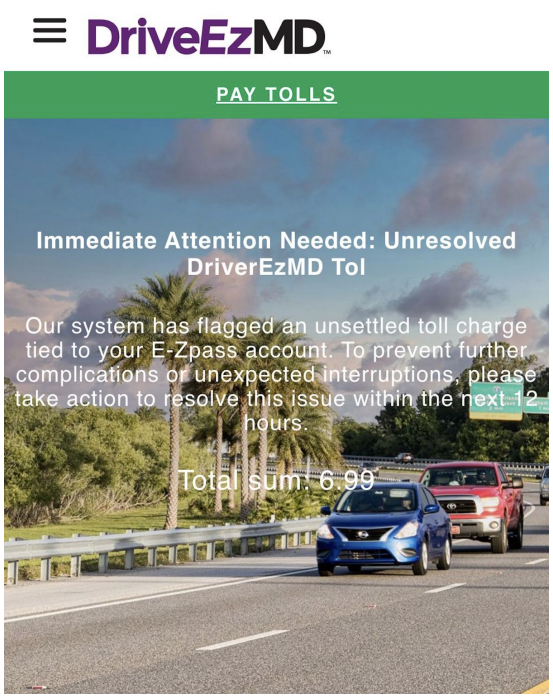
- **Dual deception**: Attempting to deceive potential victims and analysts alike. In isolation, reports may go undisrupted and referred to the registrant (malicious actor).

- **Effective**: Smishing combination makes it a convincing impersonation.

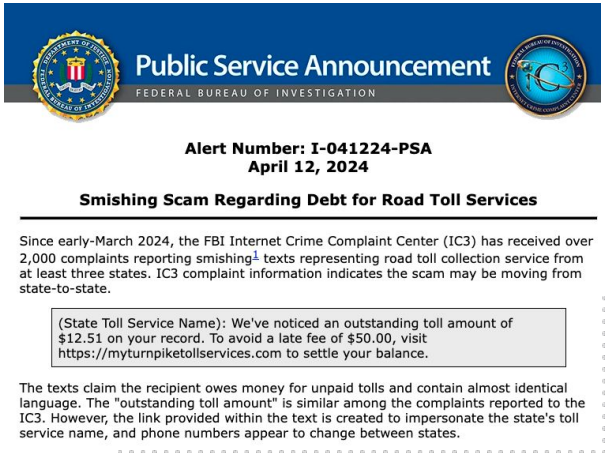
- **Not isolated**: Associated with automated campaigns. Difficult to prevent harm through reactive mitigation.

Not isolated: Toll Road Scams

https://driveezmd.com-pqsx.win/us
https://driveezmd.com-puqz.win/us
https://driveezmd.com-pxrl.win/us
https://driveezmd.com-pzbj.win/us
https://driveezmd.com-qjgm.win/us
https://driveezmd.com-qkvu.win/us
https://driveezmd.com-qlie.win/us
https://driveezmd.com-qnek.win/us
https://driveezmd.com-qnek.win/us/
https://driveezmd.com-qpjn.win/us
https://driveezmd.com-qsjx.win/us
https://driveezmd.com-qtem.win/us
https://driveezmd.com-qtxf.win/us
https://driveezmd.com-qukc.win/us
https://driveezmd.com-qvuh.win/us
https://driveezmd.com-qxyn.win/us
https://driveezmd.com-qybd.win/us
https://driveezmd.com-rcnh.win/us
https://driveezmd.com-rdvo.win/us
https://driveezmd.com-rdvo.win/us/
https://driveezmd.com-reap.win/us
https://driveezmd.com-rfgc.win/us
https://driveezmd.com-rgvk.win/us
https://driveezmd.com-rjnuh.vip/us



driveezmd.com-[xxxx].TLD



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-041224-PSA
April 12, 2024

Smishing Scam Regarding Debt for Road Toll Services

Since early-March 2024, the FBI Internet Crime Complaint Center (IC3) has received over 2,000 complaints reporting smishing[1] texts representing road toll collection service from at least three states. IC3 complaint information indicates the scam may be moving from state-to-state.

> (State Toll Service Name): We've noticed an outstanding toll amount of $12.51 on your record. To avoid a late fee of $50.00, visit https://myturnpiketollservices.com to settle your balance.

The texts claim the recipient owes money for unpaid tolls and contain almost identical language. The "outstanding toll amount" is similar among the complaints reported to the IC3. However, the link provided within the text is created to impersonate the state's toll service name, and phone numbers appear to change between states.

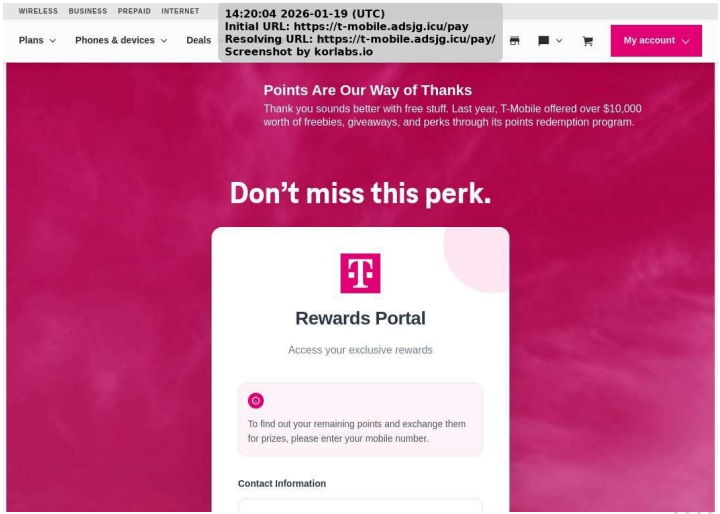
FBI Warning
https://www.ic3.gov/PSA/2024/PSA240412

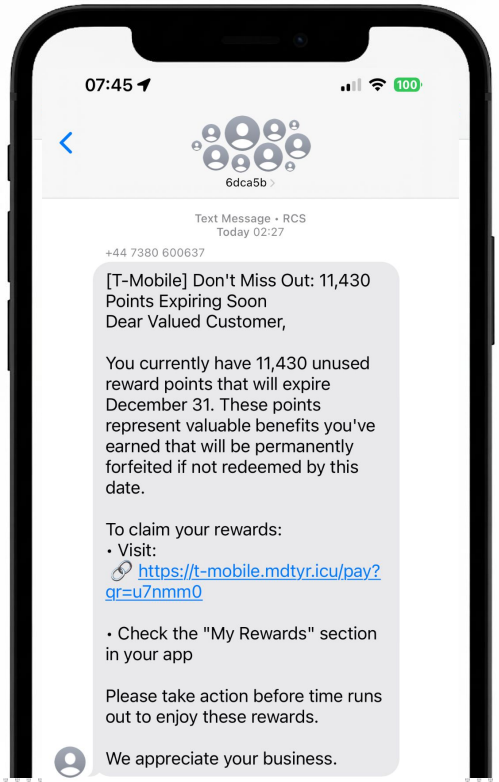
Not isolated: Mobile Smishing

http://t-mobile.com-fqam.top/pay
http://t-mobile.com-hbs.cc/pay
http://t-mobile.com-nsa.shop/us
http://t-mobile.com-sjl.top/
http://t-mobile.com-snr.top/
http://t-mobile.com-sto.top/
http://t-mobile.com-suqq.cc/pay
http://t-mobile.com-swr.top/
http://t-mobile.com-szn.top/
http://t-mobile.com-taq.top/
http://t-mobile.com-xrw.com/pay?CIRJ=egjhEw
http://t-mobile.com-xxsw.cc/pay
http://t-mobile.cpoaw.cc/pay/
http://t-mobile.cuwgm.cc/pay/
http://t-mobile.cvrdj.icu/pay
http://t-mobile.cxvth.icu/pay
http://t-mobile.czayw.cc/pay/
http://t-mobile.dayno.cc/pay/
http://t-mobile.dgrue.cc/pay/
http://t-mobile.dmxnk.icu/pay/
http://t-mobile.dpbli.cc/pay/
http://t-mobile.dqkzu.cc/pay/
http://t-mobile.dspco.cc/pay/
http://t-mobile.dtcxh.cc/pay/
http://t-mobile.duinw.icu/pay/

t-mobile.com-[xxxxx].TLD

t-mobile.[xxxxx].TLD

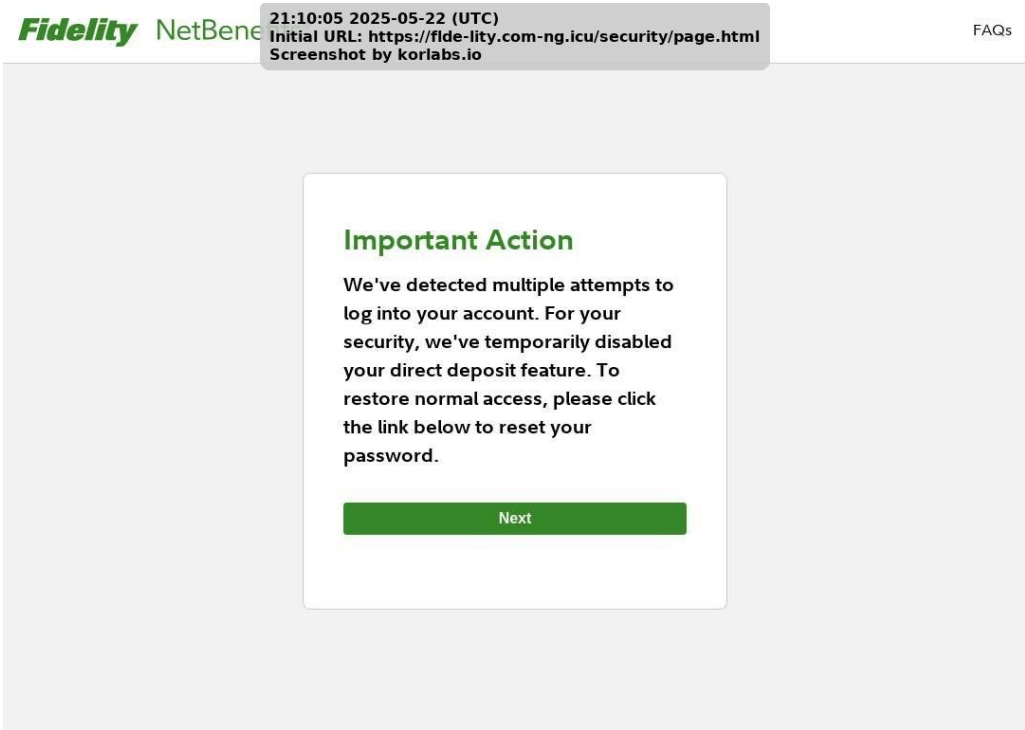




Not isolated: Fidelity Investments

fide-lity.com-[xx].TLD

http://flde-lity.com-ni.bond/security/page.html	com-ni.bond
http://flde-lity.com-nk.cyou/security/page.html	com-nk.cyou
http://flde-lity.com-nk.icu/security/page.html	com-nk.icu
http://flde-lity.com-nl.cyou/security/forgotLogin...	com-nl.cyou
http://flde-lity.com-nl.qpon/security/forgotLogin...	com-nl.qpon
http://flde-lity.com-nn.cyou/security/page.html	com-nn.cyou
http://flde-lity.com-no.cyou/security/page.html	com-no.cyou
http://flde-lity.com-no.qpon/security/forgotLogin...	com-no.qpon
http://flde-lity.com-nr.cyou/security/page.html	com-nr.cyou
http://flde-lity.com-nr.icu/security/page.html	com-nr.icu
http://flde-lity.com-ns.cyou/security/page.html	com-ns.cyou
http://flde-lity.com-ns.icu/security/forgotLogin.ht..	com-ns.icu
http://flde-lity.com-ns.qpon/security/page.html	com-ns.qpon
http://flde-lity.com-nu.bond/security/forgotLogin...	com-nu.bond
http://flde-lity.com-nu.cyou/security/forgotLogin...	com-nu.cyou
http://flde-lity.com-nu.icu/security/page.html	com-nu.icu
http://flde-lity.com-nu.qpon/security/forgotLogin...	com-nu.qpon
http://flde-lity.com-nv.icu/security/forgotLogin.ht..	com-nv.icu



Why care? Continued…
Incomplete Reports

uk-winteruol.qpon
uk-winteruoo.qpon
uk-winteruop.qpon
uk-winteruoq.qpon
uk-winteruor.qpon
uk-winteruow.qpon
uk-winteruti.qpon
uk-winterutk.qpon
uk-winterutp.qpon
uk-winterutq.qpon
uk-winterutr.qpon

https://gov.uk-winteruol.qpon/uk
https://gov.uk-winteruoo.qpon/uk
https://gov.uk-winteruop.qpon/uk
https://gov.uk-winteruoq.qpon/uk
https://gov.uk-winteruor.qpon/uk
https://gov.uk-winteruow.qpon/uk
https://gov.uk-winteruti.qpon/uk
https://gov.uk-winterutk.qpon/uk
https://gov.uk-winterutp.qpon/uk
https://gov.uk-winterutq.qpon/uk
https://gov.uk-winterutr.qpon/uk

Often report providers/feeds don't capture the complete URL.

Making it hard to:

- Collect screenshots
- Measure mitigation
- Action the report

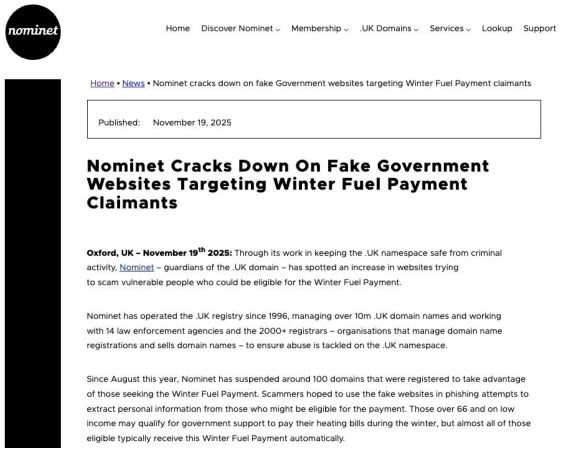
Practical steps

- Registrars and registries should be aware of this trend and look out for ‘TLD-’ combinations, for example: **com-**, **uk-, gov-, de-, ca-, org-, pl-** etc. or **-uk, -com, -gov** etc.
- Highlights the importance of Associated Domain Check in unearthing automated malicious campaigns.
  - PDP
  - Voluntary process changes

More information

https://netbeacon.org/bulletin-dns-abuse-campaign-exploiting-subdomain-cloaking

https://nominet.uk/blog/criminals-are-exploiting-the-uks-winter-fuel-payment-this-is-how-global-industry-collaboration-is-tackling-it/



https://nominet.uk/news/nominet-cracks-down-on-fake-government-websites-targeting-winter-fuel-payment-claimants/

Thank you! Questions?