TLP:CLEAR

CYBERSHIELD
ASOCIATIA EDUCATIE IN SECURITATE CIBERNETICA

RAPORT THREAT INTELLIGENCE

Escrocheria cu reînnoirea falsă a domeniilor

Un singur operator rulează o rețea multi-brand, multi-țară de site-uri false de „reînnoire / protecție domenii” care facturează firme pentru un serviciu pe care nu l-au cumpărat și de care nu au nevoie. Traficul e ascuns prin Cloudflare, iar toate site-urile sunt servite de pe o singură gazdă.

65+ domenii frauduloase · 8+ familii de brand · ~20 de țări · o singură origine cPanel

DRNS | DMS | DNRS | DRM | IDS | IDM | branduri „renewal” & „recovery”

ELABORAT DE
CyberShield, Asociația Educație în Securitate Cibernetică

DATA
11 septembrie 2026

REFERINȚĂ
CS-TI-2026-0911-DRNS-RO

CONTACT
contact@cybershield.org

1 · Rezumat

Prezentul raport documentează o operațiune de fraudă activă și organizată care vizează firme mici și mijlocii prin **facturi false de reînnoire a domeniilor**. Operatorul înregistrează domenii „naționale” care imită un serviciu legitim (de exemplu `dmsromania.com`, `drnsromania.com`), le îmbracă în aparența unei firme de înregistrare / protecție a domeniilor și trimite firmelor o factură urgentă pentru a „reînnoi” sau „proteja” un domeniu cu care nu are absolut nicio legătură. Cine plătește nu primește nimic de valoare; înregistrarea reală a domeniului rămâne neatinsă, la registratorul legitim.

Concluzii cheie

- CONFIRMAT **Un singur operator, multe măști.** Istoricul de certificate (Certificate Transparency) al platformei-backend `drnsglobal.org` (**509 certificate**) scoate la iveală **peste 65 de domenii frauduloase**, în cel puțin **8 familii de brand**, DRNS, DMS, DNRS, DRM, IDS, IDM, branduri generice de tip „renewal” și chiar fațade de tip „recovery” / recuperare creanțe, care acoperă ~20 de țări. **Toate** se rezolvă către o singură origine, `206.168.149.10` (o gazdă cPanel partajată), prin `<domeniu>.drnsglobal.org`. Lista completă în Anexa A.
- CONFIRMAT **Fenomen deja documentat internațional.** Furnizori de găzduire și registratori naționali au publicat avertizări despre aceeași rețea, sub brandurile ei de țară, **DNRS Australia**, **DMS Australia**, **DRM Australia** (Conetix), **DMS Finland** (Hostaan), **IDS Ireland** (webworld.blog), **DNRS UK** (89 GBP) și **DRNS New Zealand**, descris de un furnizor drept „o franciză internațională de escrocherii”.
- CONFIRMAT **Cloudflare ascunde originea** și furnizează certificate TLS gratuite. Două perechi de nameservere Cloudflare (`jerome/lola` și `fiona/ken`) sunt folosite alternativ, peste ambele branduri și ambii registratori, semn de conturi Cloudflare multiple aparținând aceluiași actor.
- PREJUDICIU **Oamenii plătesc.** Facturile sunt mici și localizate, **433 RON** (România), **89 GBP** (Marea Britanie), **182 AUD** (Australia), gândite să treacă neobservate prin contabilitate. „Serviciul” vândut, un *serviciu de notificare a reînnoirii domeniului*, este intenționat lipsit de valoare, ales astfel încât operatorul să poată susține că nu se dă drept registrator.

De ce am investigat

Ni s-a semnalat faptul că **mai mulți deținători de domenii din România** au primit astfel de e-mailuri de „reînnoire”. Pornind de la un caz concret (o firmă din România a primit o factură de 433 RON de la `dmsromania.com` pentru un domeniu `.ro` gestionat de cu totul alt registrator, cu o dată de expirare inventată), am început să investigăm în amănunt. Rezultatul este cartografierea completă a rețelei, prezentată mai jos.

2 · Cum funcționează frauda

Este o variantă modernă și localizată a vechii înșelătorii de tip „conflict de domeniu / nume de companie” și „reînnoire falsă de domeniu”, asociată istoric cu operatori-fantomă din Hong Kong / China continentală. Evoluția din 2025-2026 adaugă site-uri convingătoare pe fiecare țară și pagini de plată cu cardul.

1. Recoltare
Țința și domeniul, extrase din WHOIS public / registre de firme

→

2. Factură
„Reminder prietenos” nesolicitat, cu dată și sumă inventate

→

3. Presiune
Termen scurt; „neplata duce la dezactivarea serviciului”

→

4. Colectare
„View Invoice” → card / Apple / Google Pay pe `account.<domeniu>`

2.1 Exemplu documentat, România (datele victimei anonimizate)

Un mesaj real primit în septembrie 2026 de o firmă de arhitectură/construcții din România. **Numele firmei și domeniul exact sunt redactate**; restul elementelor sunt reproduse ca atare, inclusiv greșelile de scriere ale operatorului.

> De la: „David Lee" <info@dmsromania.com> · Subiect: domain renewal reminder
>
> Dear [redacted] team,
>
> This is a friendly reminder that **invoice 3192195 for 433.00 RON** is due on **10/Sep/2026**. We would like you to extend the **domain renewal notification service** for the domain below:
>
> **Domain:** www.[redacted].ro · **Amount due:** 433.00 RON · **Renewal date:** 10/Sep/2026
>
> To keep your domain **renwal** notification service active without interruption, please complete payment now. **[View Invoice]**
>
> **Note: Non-payment will result in deactivation of service.**
>
> Best regards
> David Lee, **DMS Romania**, Calea Floreasca 169A, #06-01, București 077190, Romania, info@dmsromania.com

De ce este fraudulos acest mesaj, element cu element

Element observat	De ce este fraudulos / semnal de alarmă
„domain **renewal notification** service"	Un „produs" inventat și fără sens. Expeditorul **nu este registratorul** și nu poate reînnoi domeniul. Formularea este o portiță deliberată: vând „notificări", nu înregistrare, ca să estompeze impersonarea. Aceeași formulare apare identic în variantele din Australia, Marea Britanie și Finlanda (§9).
Dată și sumă **inventate**	`10/Sep/2026` și `433 RON` nu corespund datei reale de expirare, care este deținută de registrul `.ro` (ROTLD / ICI București) prin registratorul real al firmei. Cifrele sunt inventate ca să creeze urgență.
Nicio relație anterioară	Victima nu a contractat niciodată această entitate. Domeniul real folosește alt registrator și alte nameservere; „DMS Romania" nu apare nicăieri în evidențele legitime.
Urgență + amenințare	„Non-payment will result in deactivation of service", presiune ca destinatarul să plătească înainte să verifice.
Adresă contradictorie / imposibilă	Semnătura dă o adresă din București folosind formatul de unitate `#06-01`, o numerotare de apartament din **Singapore** / **Hong Kong**, nu din România: o urmă de copy-paste dintr-un șablon asiatic. Site-ul aceluiași brand afișează, în schimb, o adresă din **Hong Kong** (§4).
Persoană generică & greșeli de scriere	„David Lee" este un alias generic, de neurmărit; „**renwal**" este scris greșit, inconsecvent cu un furnizor real din România.
Plată cu cardul pe un portal-clonă	Registratorii reali reînnoiesc prin contul pe care îl ai deja. Un e-mail rece care împinge plata instant cu cardul pe `account.<domeniu>` este un semn clar de fraudă și un risc de furt al datelor de card.

Impact, de ce trebuie oprit rapid

Facturile sunt intenționat mici și „de rutină", așa că sunt frecvent **plătite fără verificare** de personalul financiar, care presupune că este factura reală a domeniului firmei. Fiecare factură plătită finanțează operațiunea și expune un card unui portal ostil. Pentru că rețeaua este șablonizată și acoperă ~20 de țări, pierderile cumulate cresc rapid, iar operațiunea este **încă în expansiune** (ultimele domenii, mai 2026).

3 · Expeditorul nu are nicio legătură cu domeniul real

În exemplul documentat, domeniul `.ro` legitim al victimei este gestionat în întregime în afara acestei rețele, reprezentativ pentru fiecare caz din campanie.

	Domeniul real (legitim)	Ce pretinde escrocheria
Registru / registrator	ROTLD (ICI București) prin registrator `.ro` acreditat (observat: `ICI - Registrar`; nameservere `ns1/ns2.chroot.ro`)	„DMS Romania”, **nu este registrator**, nu este acreditat ROTLD, nu poate reînnoi un domeniu `.ro`
Expirare / reînnoire	Deținută de registru; reînnoită prin contul propriu de la registratorul real	Dată și taxă inventate, trimise pe e-mail
Relație de facturare	Inexistentă cu DMS/DRNS	„Factura 3192195” fabricată

4 · Identitate & impersonare

Operatorul prezintă **cel puțin trei identități care se contrazic reciproc** pentru ceea ce, demonstrabil, este aceeași infrastructură, inconsecvență care este ea însăși o dovadă puternică de fraudă.

Suprafață	Identitate pretinsă	Detaliu / problemă
Site-uri (`drnsglobal.org` ș.a.)	**DRNS Global**, Hong Kong	„Unit B, 11/F Yam Tze Commercial Building, 23 Thomson Road, Wan Chai”; „BRN: 74404086”; doar e-mail, fără telefon, fără persoane. Clădirea din Wan Chai este o adresă cunoscută de tip birou virtual, prezentă în baza **ICIJ Offshore Leaks**. BRN-ul afișat nu a putut fi asociat unei firme active printr-o căutare publică.
E-mailurile de factură	**DMS Romania**, București	„Calea Floreasca 169A, #06-01, București 077190”, numerotare asiatică lipită într-o adresă românească; nicio firmă cu acest nume nu este înregistrată acolo.
Subsol de site	**DRNS Africa** (`info@drnsafrica.com`)	Un al treilea brand regional, referit ca un contact „vechi”, același șablon reutilizat pe regiuni.
Branduri pre-poziționate	**DRNS UK**, DRNS Sweden/ Denmark/Finland	Înregistrate, dar parcate (`127.0.0.127`), branduri de țară pregătite pentru activare ulterioară, inclusiv o identitate britanică.

Impersonare de categorie

Site-urile se prezintă cu vocabularul unor firme legitime de **protecție a brandurilor** / **domeniilor**, „protecția identității digitale”, „administrarea portofoliului de domenii”, „recuperarea proprietății”, „apărare împotriva transferurilor neautorizate”, împrumutând astfel credibilitatea unei industrii reale, fără nicio acreditare, entitate, listă de prețuri, testimoniale sau istoric. Site-urile nu au **niciun preț, niciun număr de clienți, nicio acreditare ICANN și niciun logo de partener**. Aspectul există doar ca să facă o factură rece să pară plauzibilă.

4.1 O adresă falsă diferită pentru fiecare țară

Fiecare brand național publică propria adresă cu aparență locală, deși toate sunt servite de pe același backend și folosesc același șablon. Nicio firmă reală cu numele brandului nu funcționează la aceste adrese.

Brand	Adresa pretinsă pe site	Evaluare
DRNS Global	Unit B, 11/F Yam Tze Commercial Building, 23 Thomson Road, Wan Chai, **Hong Kong**; BRN 74404086	Clădire de tip birou virtual (în ICIJ Offshore Leaks); BRN neasociat unei firme active la o căutare publică.

DMS Ireland	Alexandra House, Ballsbridge Park 3, Suite 814, **Dublin** D04 C7H2	Adresă de tip birou-serviciu / virtual; același șablon ca site-ul din Hong Kong.
DMS Romania	Calea Floreasca 169A, #06-01, **București** 077190 (în semnătura e-mailului)	Folosește formatul de unitate Singapore/HK „#06-01”; nicio firmă înregistrată.
Altele	Branduri pe țări (Italia, Spania, Polonia, Finlanda…), fiecare cu o pagină locală	Aceeași platformă, același design, alt nume de țară.

5 · Infrastructura tehnică

În ciuda brandurilor, registratorilor și conturilor Cloudflare multiple, întreaga rețea se reduce la **o singură platformă backend**. Acesta este nucleul dovezilor.

5.1 O singură platformă backend, `drnsglobal.org`

Fiecare site public este un „virtual host” servit prin reverse-proxy de pe o singură origine, dovedit în două moduri independente:

- **Certificate Transparency.** Certificatele TLS ale domeniilor publice conțin intrări SAN de forma `<domeniu>.drnsglobal.org` și wildcard-urile `*.com/.net/.org.drnsglobal.org`, de ex. `drnsromania.com.drnsglobal.org`, `www.dmsromania.com.drnsglobal.org`.
- **DNS direct.** Fiecare astfel de nume se rezolvă către o singură origine, `206.168.149.10`; câteva domenii (`idsgroupltd.net`, `drnsnz.org`) se rezolvă direct acolo, ocolind Cloudflare.

Domeniu / platformă backend	`drnsglobal.org` (și hub de brand)
IP de origine	`206.168.149.10`
Gazdă de origine	**RackNerd LLC** (SUA, Los Angeles), DNS invers `fiber17-r.iaasdns.com`
Nameservere de origine	`ns1.iaasdns.com`, `ns2.iaasdns.com` (găzduire partajată iaasDNS)
Natura originii	Un singur **cont cPanel partajat** (expune `cpanel./webmail./autodiscover.drnsglobal.org`); serverul are mulți alți chiriași fără legătură, deci acțiunea vizează **contul drnsglobal.org**, nu tot IP-ul.
Volum de certificate	**509** certificate în CT pentru `*.drnsglobal.org`, aproximativ unul per domeniu-victimă (Anexa A).
Mail backend	SPF `+ip4:206.168.149.10 include:relay.mailbaby.net` (releu SMTP Mail Baby)

5.2 Ascunderea prin Cloudflare

Site-urile publice își ascund originea în spatele Cloudflare, care furnizează și certificatele TLS (DV). Două perechi de nameservere sunt folosite **alternativ, peste ambele branduri și ambii registratori**, cel mai puternic indiciu că un singur actor controlează totul:

Pereche NS Cloudflare	Intervale IP proxy observate	Folosită de (amestecat între branduri)
`jerome.ns.cloudflare.com` `lola.ns.cloudflare.com`	`104.21.x`, `172.67.x`, `188.114.96/97.8`	drnsromania, drnsitaly, drnsspain, drnsjapan, drnsglobal.com, drnsafrica.com, drnseurope.com, **dmsdenmark, dmsfinland**
`fiona.ns.cloudflare.com` `ken.ns.cloudflare.com`	`104.21.x`, `172.67.x`	dmsromania, dmspoland, dmsireland, **drnsafrica.org**

Folosirea încrucișată (un domeniu „DMS” pe perechea NS „DRNS” și invers) leagă cele două branduri de un singur operator.

5.3 Registratori, deținători & mail

Atribut	Profil brand DRNS	Profil brand DMS
Registrator	**NICENIC INTERNATIONAL GROUP** (Hong Kong; IANA 3765)	**GoDaddy.com, LLC** (IANA 146)
Deținător (WHOIS privacy)	Organizație goală · Stat „**Panama City**” · țara **PA**	**Domains By Proxy, LLC** · **Arizona, SUA**
Mail	Releu Mail Baby prin originea RackNerd	**Microsoft 365** (`*.mail.protection.outlook.com`) + GoDaddy `secureserver.net` ; SPF de trimitere prin **HostPapa** `107.161.89.109/189/19/190/191` ; DMARC `p=quarantine` , `rua@onsecureserver.net`
Token-uri M365	,	`MS=ms71420813` (dmsromania), `MS=ms27114960` (dmspoland)
DNSSEC	Nesemnat	Nesemnat

5.4 Cum sunt făcute site-urile și cum se încasează plata

Site-urile publice sunt construite în **WordPress** (jQuery / JQMIGRATE observate) și folosesc același șablon de prezentare. Butonul „View Invoice / Pay online” duce la o pagină de plată găzduită pe subdomeniul `account.<domeniu>` , care rulează **Invoice Ninja**, o aplicație open-source de facturare pe care operatorul o folosește ca să genereze facturile false și să încaseze plăți cu cardul (Visa, Mastercard, Apple Pay, Google Pay). Pagina de autentificare cere **e-mail, parolă, un cod 2FA și un „secret”** (capturi în Anexa B). Este, în același timp, un canal de fraudă financiară și un mijloc prin care ți se pot fura datele de autentificare.

6 · Evaluarea atribuirii

Evaluare: un singur operator, încredere ridicată. Legăturile independente converg:

1. **Backend comun**, toate site-urile publice trec prin proxy către `206.168.149.10` via `*.drnsglobal.org` (CT + DNS).
2. **Cod de platformă comun**, șablon de site identic la toate brandurile; site-urile DMS poartă chiar intrări SAN `<domeniu>.drnsglobal.org` , adică DMS este găzduit pe platforma DRNS.
3. **Conturi Cloudflare interschimbabile**, cele două perechi NS sunt amestecate între branduri și registratori.
4. **Mod de operare consecvent**, WHOIS privacy, DNSSEC nesemnat, fără telefon, un singur e-mail generic, identități HK/RO inventate, aceeași structură și formulare a e-mailului de fraudă în toate țările.
5. **Cronologie coordonată**, înregistrări în masă, în ferestre strânse, câteva create în aceeași secundă (§8).

6.1 Piste de atribuire

- **„praveen1”.** Pe platformă apare și adresa `praveen1.duckdns.org` , care se rezolvă tot către originea `206.168.149.10` . Astfel de adrese sunt oferite gratuit de serviciul DuckDNS și sunt create manual de o persoană, iar de obicei indică chiar serverul acelei persoane. Este o pistă către un administrator care folosește numele „praveen1”.
- **Cont cPanel partajat.** Platforma expune `cpanel./webmail./autodiscover./autoconfig./webdisk./cpcalendars./cpcontacts` , întreaga rețea rulează într-**un singur cont cPanel** pe serverul RackNerd/iaasDNS. Acel cont este veriga centrală.
- **Origini expuse direct.** `idsgroupltd.net` și `drnsnz.org` se rezolvă direct către `206.168.149.10` , confirmare independentă a backend-ului comun.

7 · Inventar (indicatori prioritari)

Tabelul A, Site-uri frauduloase confirmate (active, pe platforma comună) CONFIRMAT

Toate se rezolvă către originea `206.168.149.10` via `<domeniu>.drnsglobal.org` și sunt ascunse prin Cloudflare. Fiecare expune și un portal de plată la `account.<domeniu>`.

Domeniu	Brand	Registrator	Creat	Pereche NS CF	Mail
`drnsromania.com`	DRNS	NICENIC	2025-12-19	jerome/lola	,
`drnsitaly.com`	DRNS	NICENIC	2025-12-19	jerome/lola	,
`drnsspain.com`	DRNS	NICENIC	2025-12-19	jerome/lola	,
`drnsjapan.com`	DRNS	NICENIC	2025-12	jerome/lola	,
`dmsromania.com`	DMS	GoDaddy	2026-02-13	fiona/ken	M365 + HostPapa
`dmspoland.com`	DMS	GoDaddy	2026-05-08	fiona/ken	M365 + HostPapa
`dmsireland.com`	DMS	GoDaddy	2026-01-24	fiona/ken	M365
`dmsdenmark.com`	DMS	GoDaddy	2026-01-24	jerome/lola	M365
`dmsfinland.com`	DMS	GoDaddy	2026-02-13	jerome/lola	M365
`drnsafrica.org`	DRNS Africa	NICENIC	2025-11-14	fiona/ken	M365

Tabelul B, Domenii-hub / coloana vertebrală CONFIRMAT

Domeniu	Rol	Registrator	Creat	Găzduire
`drnsglobal.org`	**Platformă backend** + hub	NICENIC	2025-11-26	RackNerd `206.168.149.10` (direct)
`drnsglobal.com`	Hub de brand (cel mai vechi)	NICENIC	2025-10-31	Cloudflare (jerome/lola)
`drnsafrica.com`	Hub regional	NICENIC	2025-11-06	Cloudflare (jerome/lola)
`drnseurope.com`	Hub regional	NICENIC	2025-10-31	Cloudflare (jerome/lola)

Tabelul C, Indicatori (IOC) consolidați

Tip	Valoare
IP de origine (backend)	`206.168.149.10` (RackNerd LLC; rDNS `fiber17-r.iaasdns.com`)
Platformă backend	`drnsglobal.org`; tipar SAN `<domeniu>.drnsglobal.org`, `*.com/.net/.org.drnsglobal.org`
Nameservere de origine	`ns1.iaasdns.com`, `ns2.iaasdns.com`
Perechi NS Cloudflare	`jerome+lola.ns.cloudflare.com`; `fiona+ken.ns.cloudflare.com`
Registratori	NICENIC INTERNATIONAL GROUP (IANA 3765); GoDaddy (IANA 146) + Domains By Proxy
E-mailuri de contact	`info@drnsglobal.org`, `info@drnsafrica.com`, `info@dmsromania.com`
Infrastructură mail	`relay.mailbaby.net`; `*.mail.protection.outlook.com`; SPF HostPapa `107.161.89.109/189/19/190/191`; `include:secureserver.net`
Artefact de atribuire	`praveen1.duckdns.org` → `206.168.149.10`

Adrese pretinse	HK: „Yam Tze Commercial Building, 23 Thomson Road, Wan Chai” (BRN 74404086) · RO: „Calea Floreasca 169A, #06-01, București”
Persoană / portaluri	„David Lee” · portaluri de plată `account.<domeniu>` (Invoice Ninja)

8 · Cronologia înregistrărilor

Gruparea strânsă, inclusiv domenii create în **aceeași secundă**, indică o provizionare automată și coordonată, nu o creștere organică.

Data (UTC)	Active înregistrate	Interpretare
2025-10-31	`drnsglobal.com`, `drnseurope.com`	Startul operațiunii (domeniile principale de brand).
2025-11-06 / 11-14	`drnsafrica.com`, `drnsafrica.org`	Adăugarea brandului Africa.
2025-11-26	`drnsglobal.org`	**Platforma backend** ridicată pe RackNerd.
2025-12-15 → 12-19	`drnsuk.com`; apoi `drnsromania.com`, `drnsitaly.com`, `drnsspain.com`, `drnsjapan.com`	Lansarea DRNS pe țări + placeholder UK.
2026-01-24	`dmsireland.com`, `dmsdenmark.com`	**Lansarea brandului DMS** (ramura GoDaddy).
2026-02-13	`dmsromania.com`, `dmsfinland.com`, `idsromania.com`	România, vizată sub brandurile DMS și IDS.
2026-05-08	`dmspoland.com`	Expansiunea continuă, operațiunea este **activă**.

9 · Confirmare independentă (o campanie internațională documentată)

Aceeași operațiune a fost deja semnalată public de furnizori de găzduire și registratori naționali, sub brandurile ei de țară. Aceste raportări independente descriu un **mod de operare identic**, un „serviciu de notificare a reînnoirii” inventat, date de deținător recoltate, un termen scurt și aceleași metode de plată cu cardul / portofel digital, confirmând că și cazul românesc documentat aici este un nod al unei rețele mai largi. Un furnizor o numește direct „**o franciză internațională de escrocherii**”.

Țară / brand	Sursă	Detaliu cheie
Australia DNRS / DMS / DRM	Conetix, „DNRS Australia Scam Email”	Facturează „domain renewal notifications” (nu reînnoire); **182,00 AUD** / 2 ani; plată prin „Visa, Mastercard, Apple Pay, Google Pay”; recoltează datele deținătorului. Numește explicit și **DMS Australia** și **DRM Australia**.
Finlanda DMS Finland	Hostaan, avertizare	Numește „**DMS Finland**” drept expeditor fraudulos, care facturează un „serviciu de notificare a reînnoirii” nesolicitat.
Irlanda IDS Ireland	webworld.blog, alertă (feb. 2026)	E-mailuri frauduloase de reînnoire de la „**IDS Ireland**” (corespunde `idsireland.com/.org/.eu` de pe platformă).
Marea Britanie DNRS UK	Raportări din industrie	„DNRS UK” (`dnrsuk.com`) facturează firmelor britanice **89 GBP**; folosește date din WHOIS și Companies House; factură falsă cu termen de 5 zile.
Noua Zeelandă DRNS NZ	MyHost.nz · SiteHost.nz	„Domain Notifications | DRNS New Zealand”, semnalat ca escrocherie ce vizează deținători `.nz`.

Categorie globală	Safenames (dec. 2025)	Ghid despre „Chinese domain registration scam”, categoria-părinte, cu o cronologie ce se potrivește lansării acestei rețele.

Cloudflare a semnalat deja o parte din rețea

La momentul redactării, `dmspoland.com` afișează deja interstițialul propriu Cloudflare **„Suspected Phishing”** („This website has been reported for potential phishing”; Cloudflare Ray ID `a391ae776e84ca25`, Anexa B, Fig. B-5). Pentru că fiecare domeniu din Tabelele A/B și Anexa A este **același operator pe același backend**, aceeași concluzie se aplică întregii rețele.

10 · Recomandări pentru deținătorii de domenii

- Tratați orice e-mail de la aceste domenii ca fraudă. **Nu plătiți** și **nu introduceți date de card** pe paginile lor.
- Reînnoirea domeniului se face **doar** prin registratorul la care l-ați înregistrat, nicăieri altundeva. Verificați direct în contul dvs.
- Pentru domenii `.ro`, sursa de adevăr este registrul **ROTLD (ICI București)** și registratorul dvs. acreditat.
- Semnalați e-mailurile la **DNSC** (Directoratul Național de Securitate Cibernetică, `alerts@dnsc.ro`), iar dacă ați pierdut bani, sesizați Poliția Română.
- Instruiți departamentul financiar: o factură mică și „de rutină” de la un expeditor necunoscut este exact tiparul acestei fraude.

11 · Metodologie & limitări

Toate concluziile au fost obținute prin **OSINT pasiv**, WHOIS public, rezoluție DNS, jurnale Certificate Transparency, date publice de reverse-IP, avertizări publice ale terților și accesarea paginilor web publice ale operatorului. **Nu s-a efectuat nicio scanare intruzivă, nicio autentificare și niciun acces la sistemele atacatorilor.** Faptele marcate CONFIRMAT sunt verificate direct; contradicțiile de identitate combină paginile publice ale operatorului cu e-mailul furnizat de victimă. Numele și domeniul victimei sunt anonimizate. BRN-ul din Hong Kong și sumele pe alte țări decât România sunt reproduse din materialul operatorului și din raportări ale terților. Datele sunt valabile la **11 septembrie 2026**; rețeaua este activă și în evoluție.

Anexa A · Lista completă de domenii (din istoricul DNS / CT)

Următoarele domenii-victimă au fost recuperate din istoricul de Certificate Transparency al platformei-backend `drnsglobal.org` (intrări SAN de forma `<domeniu>.drnsglobal.org`). Toate sunt servite de pe o singură origine, `206.168.149.10`. Majoritatea sunt ascunse prin Cloudflare; câteva se rezolvă direct către origine.

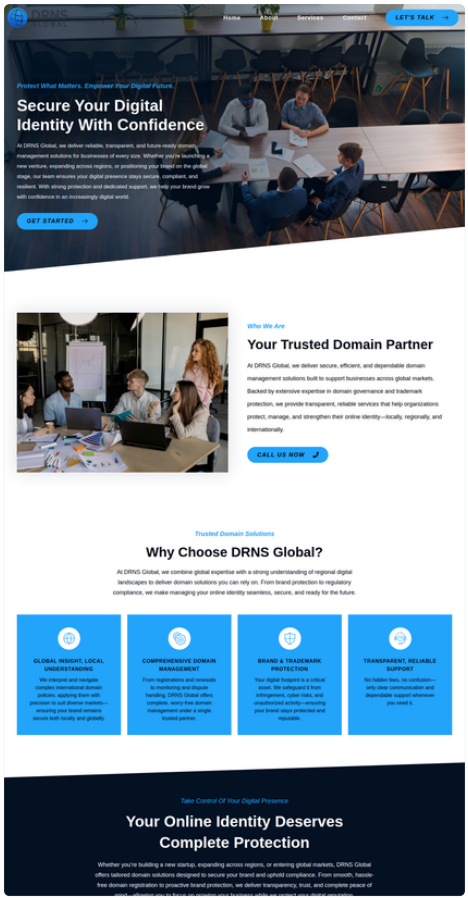
Familie de brand	Domenii
DRNS	drnsglobal.org · drnsglobal.com · drnsromania.com · drnsitaly.com · drnsspain.com · drnsjapan.com · drnseurope.org · drnsafrica.org · drnsbulgaria.org · drnsdenmark.org · drnsfinland.org · drnssweden.org · drnsuk.org · drnssk.com · drnssk.org · drnsmexico.com · drnsmx.org · drnsnewzealand.org · drnsnz.org
DMS	dmsromania.com · dmspoland.com · dmsireland.com · dmsdenmark.com · dmsfinland.com · dmsfinaland.com · dmsafrica.org · dmsaustralia.net · dmsbenelux.com · dmsbrazil.com · dmscanada.net · dmseu.com · dmsgermany.net · dmsgermany.org · dmshk.net · dmsiceland.com · dmsjapan.net · dmsnorway.net · dmsuk.org
DNRS	dnrscanada.com · dnrsnz.com · dnrsus.com · dnrsuk.com · dnrsuk.org · dnrsuk.info

DRM	`drmaustralia.com` · `drmsweden.com` · `drmswitzerland.com`
IDS	`idsgroupltd.net` · `idsireland.com` · `idsireland.eu` · `idsireland.org` · `idsromania.com` · `idsaustralia.net` · `idscanada.org` · `idseu.org` · `idsnz.com` · `idsuk.net` · `idsus.org` · `ipdscanada.com`
IDM	`idmuk.net`
Branduri „renewal”	`renewalalerts.org` · `renewalnotifications.com` · `domainsafeguard.net` · `dnsinfoltd.net`
Fațade „recovery” / creanțe	`kingswellrecovery.org` · `keystonecreditmanagement.org` · `meridiancm.org`

Notă România: pe lângă `drnsromania.com` și `dmsromania.com` (pe platformă), rețeaua deține și `idsromania.com`, un domeniu GoDaddy al cărui site nu este pe platforma comună, dar care are **același tipar de mail Microsoft 365** (`idsromania-com.mail.protection.outlook.com`), o identitate „IDS Romania” pregătită să factureze firme din România.

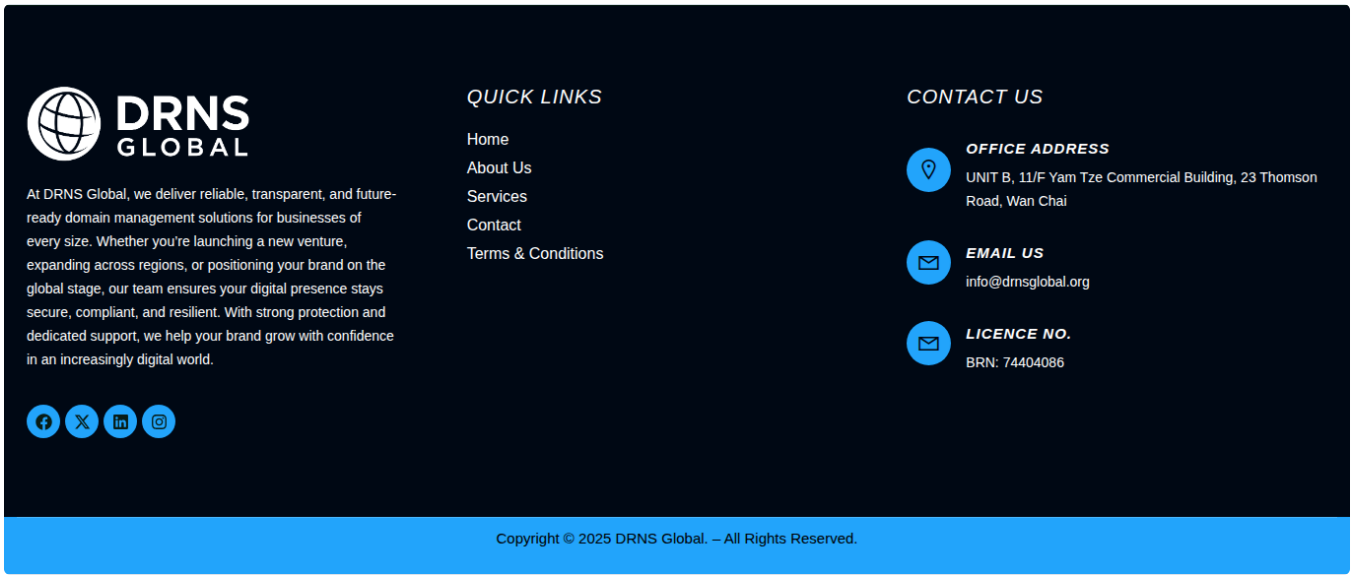
Anexa B · Dovezi vizuale (capturi live)

Capturi realizate la 11 septembrie 2026. Arată: șablonul comun reutilizat între branduri sub identități contradictorii; adresele din Hong Kong și Dublin; verdictul propriu Cloudflare de phishing pentru un domeniu al rețelei; și portalul de plată Invoice Ninja în care sunt împinse victimele.

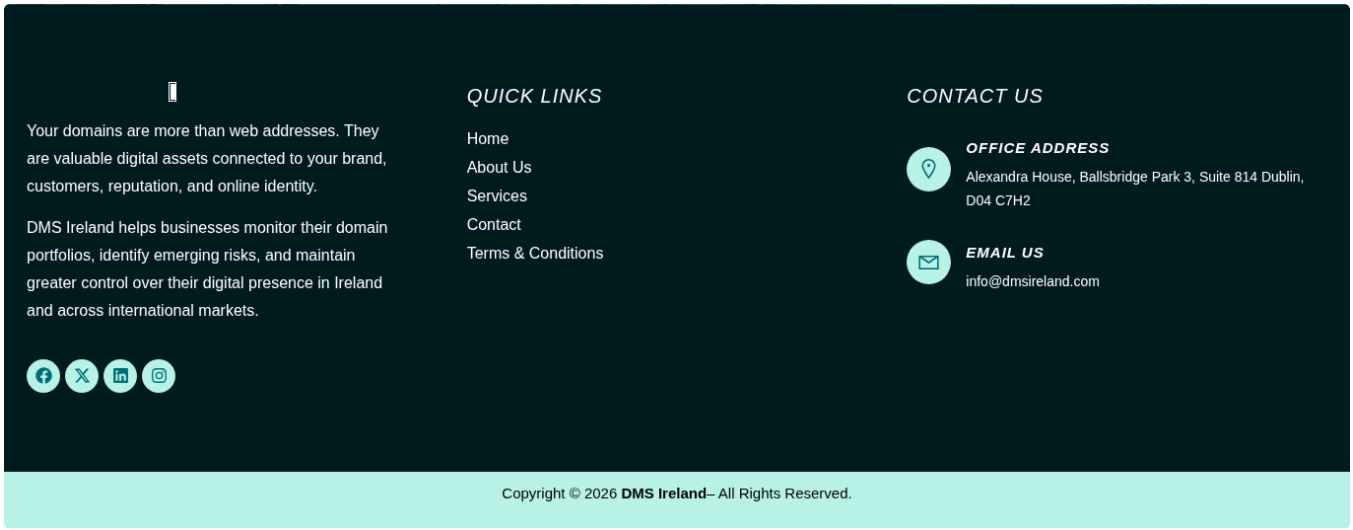


B-1 **drnsglobal.org**, hub-ul „DRNS Global”. Marketing generic de protecție a brandurilor, fără prețuri, fără acreditare, fără persoane.

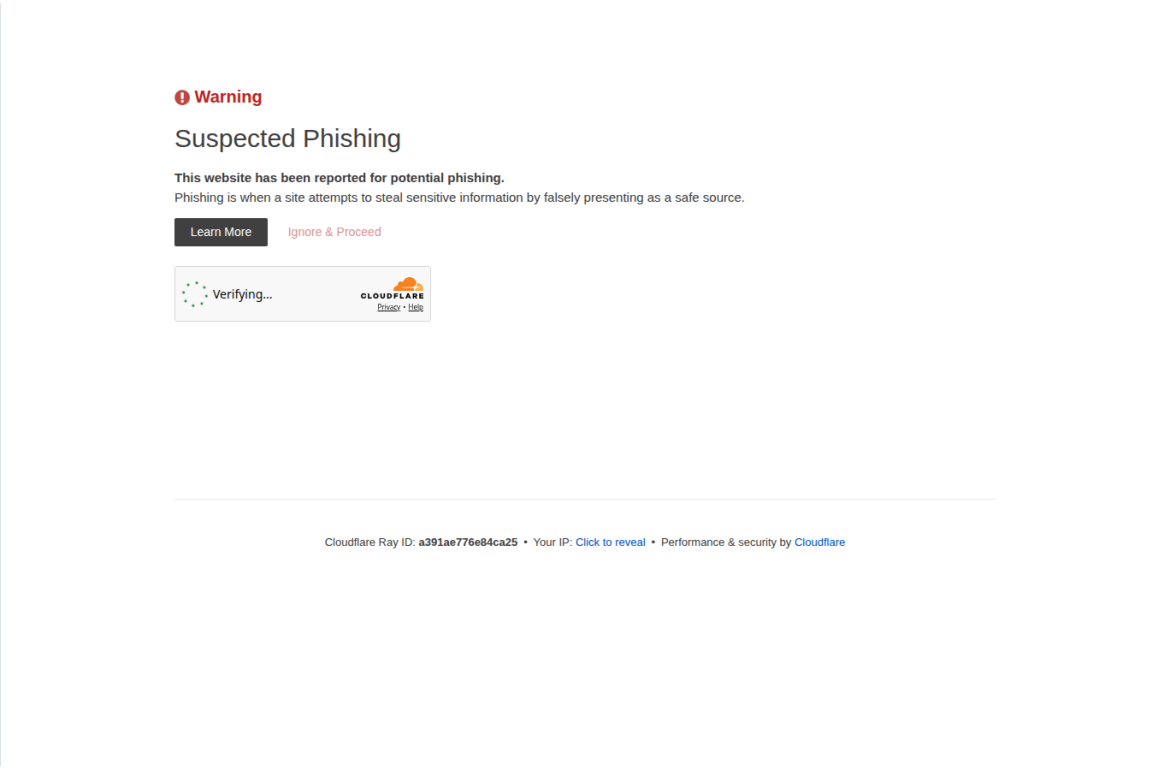
B-2 **dmsireland.com**, alt brand, **același șablon**. Aceeași platformă, altă țară.



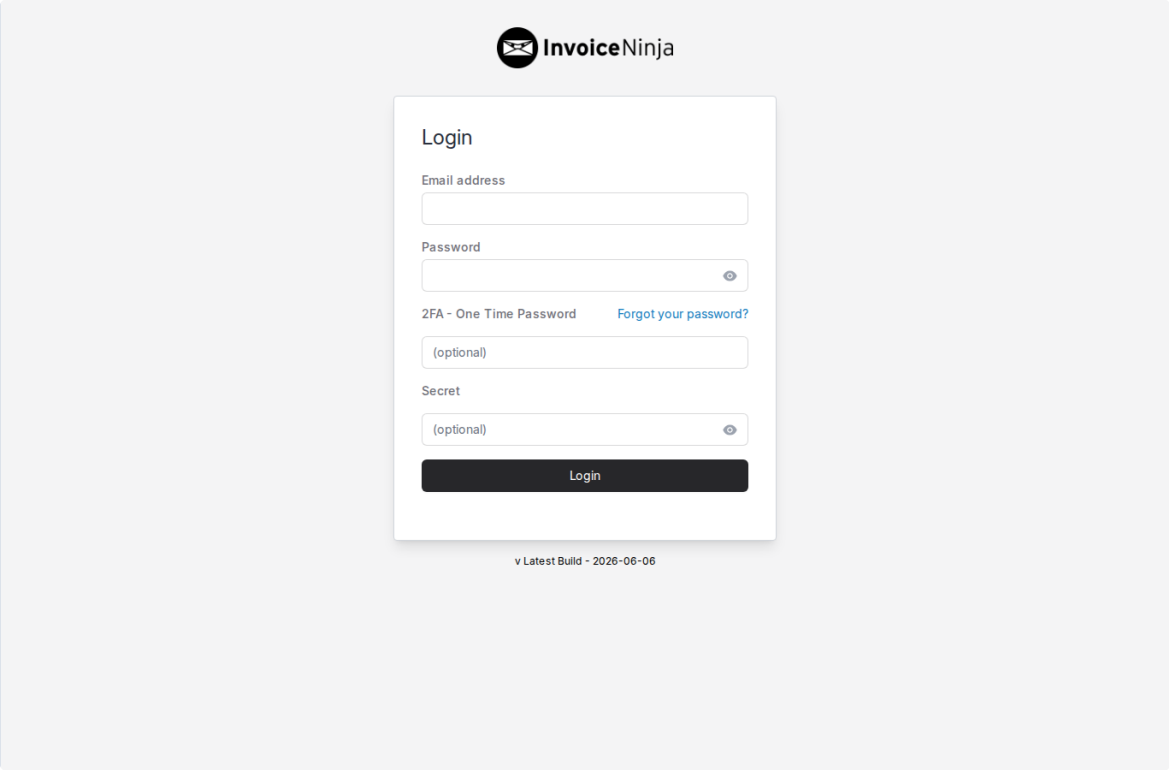
B-3 **drnsglobal.org**, subsol, adresa din Hong Kong „UNIT B, 11/F Yam Tze Commercial Building, 23 Thomson Road, Wan Chai”, `info@drnsglobal.org`, „LICENCE NO. BRN: 74404086”.



B-4 **dmsireland.com**, subsol, o adresă din **Dublin**. Altă identitate de țară pentru același operator (comparați cu B-3).



B-5 **dmspoland.com**, interstițialul propriu Cloudflare **„Suspected Phishing”**. Cloudflare Ray ID `a391ae776e84ca25`.



B-6 **account.dmspoland.com**, pâlnia de plată, o instanță **Invoice Ninja** care cere e-mail, parolă, cod 2FA și un „secret”.

CS-TI-2026-0911-DRNS-RO · Elaborat de CyberShield, Asociația Educație în Securitate Cibernetică · TLP:CLEAR, informație publică, poate fi distribuită liber în scop de prevenție și avertizare.