ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Suplantació de dominis: el cas dels *parking domains*

TLP: WHITE

MARÇ 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	27/03/2025	31/03/2025

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

La suplantació de dominis i, concretament, l'ús amb finalitats malicioses dels ***parking domains***, són temes que considerem crucials en l'àmbit de la ciberseguretat per causa de les implicacions que poden tenir a nivell dels individus i de les organitzacions.

El concepte de **suplantació de dominis** fa referència a la falsificació de llocs web o correus electrònics. Amb això es busca enganyar els usuaris per accedir a les seves dades delicades i dur a terme accions malicioses com ara la distribució de programari maliciós.

Els ***parking domains*** (o dominis d'aparcament), es fan servir específicament per dur a terme atacs de suplantació d'identitat, pesca, entre d'altres. Tot i que no hi ha una regulació específica per a aquesta mena de dominis, alguns països estan començant a abordar els riscos que comporten mitjançant lleis vinculades a la ciberseguretat i els fraus en línia.

En aquest informe s'abordarà, en primer lloc, el tema de la suplantació de dominis per després aprofundir en el cas dels *parking domains*, i com són útils per als atacants. L'auge dels *parking domains* és una tendència en el món de la cibercriminalitat. Veurem com el fet de tenir dominis «estacionats» és útil per als ciberdelinqüents. Finalment, es donaran una sèrie de recomanacions per prevenir aquests atacs tant a nivell individual com corporatiu.

3. DEFINICIONS

Tot seguit, es presenten les definicions clau per abordar la temàtica d'aquest informe:

3.1. Suplantació de dominis

3.1.1. Què és la suplantació de dominis?

La suplantació de dominis passa quan **els ciberdelinqüents falsifiquen el nom d'un lloc web o un domini de correu electrònic per tal d'enganyar els usuaris**, per fer-los creureu que són segurs. En altres paraules, els ciberdelinqüents fan creure l'usuari que està interactuant amb un lloc web legítim o un correu electrònic autèntic quan en realitat es tracta d'un intent de pesca o un atac maliciós.

Hi ha tres tipus de suplantació de dominis: de llocs web/URL, de correu electrònic i de publicitat. En aquest informe ens centrarem en la suplantació de llocs web/URL.

3.1.2. Suplantació de llocs web/URL

Suplantar un lloc web consisteix a crear un lloc web similar a un lloc web legítim, és a dir, que el lloc sembli tant al lloc original que les diferències siguin imperceptibles per a l'usuari. Per aconseguir-ho, els ciberdelinqüents fan servir les tècniques següents:

- URL similar

Amb l'objectiu de suplantar un lloc web, un atacant registra un nom de domini l'URL del qual és molt semblant, o fins i tot idèntic, al del lloc web legítim i conegut per l'usuari. La imitació de l'URL es fa mitjançant caràcters similars als reals, per exemple, faltes d'ortografia i fent servir una extensió de domini diferent (per exemple, .info en comptes de .com).

En alguns casos, als URL fraudulents es modifiquen o afegeixen caràcters comuns. Per exemple, es poden fer servir caràcters d'altres idiomes o caràcters Unicode, per tal que els usuaris no notin les diferències amb les pàgines legítimes.

Exemple:

- Legítima: www.exemple.com
- Suplantada: www.exemp ӏ e.com

  Al segon URL, la «l» ha estat reemplaçada per « ӏ », un caràcter Unicode visualment similar. Això podria enganyar els usuaris per tal que pensessin que estan visitant el lloc legítim.

- Similituds en el disseny

Per fer que el lloc fals sigui encara més creïble, l'atacant pot replicar el disseny i el text del lloc original (per exemple, el logotip, les fonts, els colors, etc.). Tanmateix, atès que alguns elements

de disseny no són fàcils d'imitar, si s'analitza molt bé la pàgina es podria detectar que el lloc web és fals.

- Sensació de seguretat

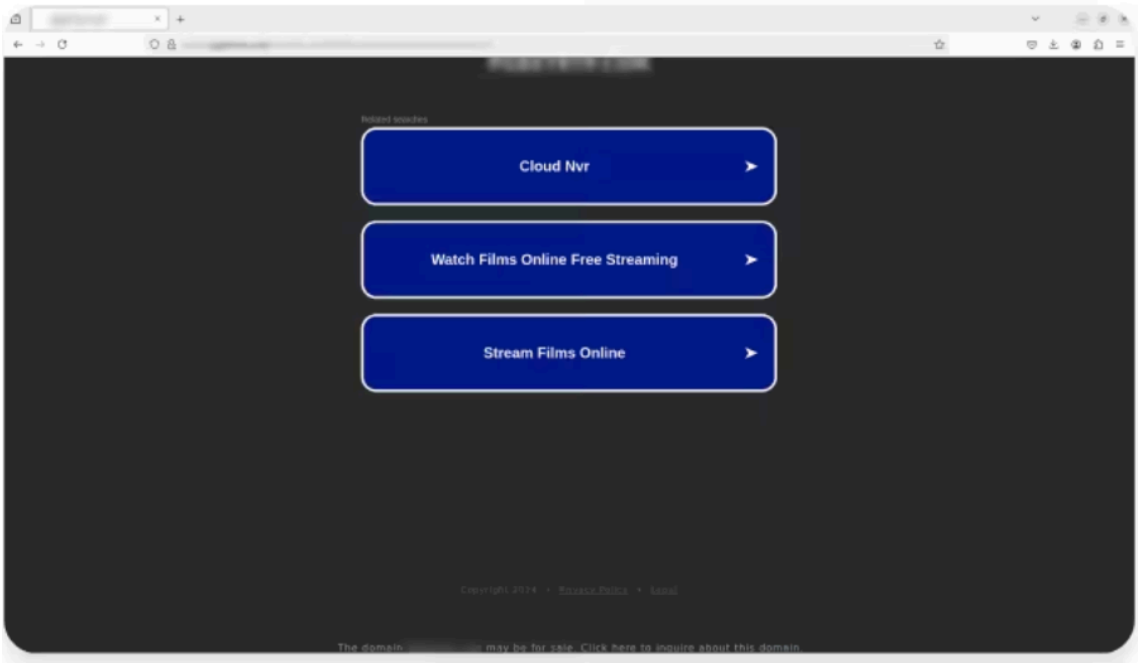
Una altra estratègia que fan servir els suplantadors és mostrar a les seves víctimes un símbol fals de connexió segura (HTTPS) per fer creure que la seva informació està xifrada, cosa que ajuda al fet que el web sembli legítim.

3.2. Els *parking domains*

Després d'haver comentat què és la suplantació de dominis, passarem a explicar el cas dels *parking domains* i com poden ser utilitzats per a finalitats malicioses, a través de la suplantació de dominis.

3.2.1. Què són els *parking domains*?

Un *parking domain* és un nom de domini que algú ha registrat i que no el fa servir de manera activa. És a dir, és qualsevol nom de domini que no està directament connectat a un lloc web o servei de correu electrònic i que tampoc redirigeix el trànsit a un altre domini amb un lloc web en funcionament.



Exemple d'un *parking domain*

3.2.2. Usos dels *parking domains* per a finalitats malicioses

Tot i que el propòsit inicial dels *parking domains* no és maliciós, aquests poden ser utilitzats de manera fraudulenta. Aquesta modalitat, que pot implicar tant la falsificació de noms de domini com la creació de llocs web amb un disseny i contingut similar a l'original, té com a objectiu robar informació confidencial, distribuir codi maliciós i/o cometre fraus publicitaris.

4. COM ELS CIBERDELINQÜENTS EXPLOTEN ELS *PARKING DOMAINS*

És freqüent que els ciberdelinqüents registrin *parking domains* i els facin servir, en el futur, per cometre delictes. És a dir, que deixen els dominis inactius durant un temps fins que els activen per a finalitats malicioses. Gràcies a això, els atacants tenen l'avantatge que el domini podria passar desapercebut fins que es faci servir per a aquestes finalitats, cosa que faria que la seva detecció inicial sigui improbable.

En els subapartats següents explicarem com es duen a terme l'ús de dominis per a finalitats malicioses, des del registre fins a l'explotació.

4.1. *Cybersquatting*

El *cybersquatting* o ciberocupació és l'acte de registrar, traficar o fer servir el nom del domini per aprofitar-se del reconeixement o prestigi que tingui una marca, sigui d'una empresa o d'una persona.

Hi ha diferents mètodes de ciberocupació, i els expliquem tot seguit:

4.1.1. *Typosquatting*

El *typosquatting* o la ciberocupació per error tipogràfic és un atac d'enginyeria social que consisteix a **registrar i fer servir dominis amb errors tipogràfics** que els usuaris podrien cometre en escriure un URL a la barra del navegador. L'atacant registra un domini que és una variació de domini legítim, mitjançant petites variacions a l'URL. Per exemple, un *typosquatter* podria registrar «facevook.com» en lloc de «facebook.com».

Els *parking domains* es presten al *typosquatting* perquè, com que no tenen contingut actiu, els atacants poden registrar dominis mal escrits o variants de dominis coneguts i després deixar aquests dominis «aparcats» fins que decideixin fer-los servir per a finalitats malicioses.

El domini registrat mitjançant el *typosquatting* i «estacionat» es pot fer servir de diverses maneres per dur a terme atacs més sofisticats. Aquests atacs poden incloure distribució de programari maliciós, pesca, suplantació d'identitat, frau publicitari, entre d'altres.

4.1.2. Registre de dominis de nom similar

En aquest cas, **es registren noms de domini que són molt similars als d'una marca** amb el mateix objectiu d'enganyar els usuaris. Es pot afegir una lletra o un prefix o sufix al nom del domini original. Per exemple, es registra «carrefouronline.es» en comptes de «carrefour.es».

4.2. Pesca i robatori d'informació

En visitar les pàgines falses que s'han activat per cometre delictes, els usuaris poden ser enganyats per tal que introdueixin informació personal, com ara contrasenyes, números de targetes de crèdit o dades bancàries. Aquests llocs de pesca poden simular pàgines web de

bancs, xarxes socials o empreses, amb l'objectiu de robar dades delicades com ara contrasenyes, dades bancàries o informació personal.

Com es fa això?

- Un atacant pot registrar un domini similar al d'una institució financera o empresa coneguda (per exemple, «exemple-secure.com» en lloc d'«exemple.com»).
- Després, redirigeix els usuaris a un lloc web fals que té el mateix disseny i contingut que l'original.
- L'atacant recopila la informació introduïda pels usuaris en el lloc fals, cosa que pot comportar un robatori d'identitat o un frau financer.

4.3. Codi maliciós o redirecció maliciosa

Alguns *parking domains* estan configurats per redirigir els usuaris a llocs maliciosos on poden ser infectats amb codi maliciós, com ara virus, troians, programari de segrest o programari espia. Aquests dominis no sempre es fan servir per a la pesca, sinó que s'empren per distribuir programari maliciós.

Com es fa això?

- L'atacant registra un domini similar al del lloc legítim i el configura per redirigir els usuaris a un lloc que disposa de contingut maliciós.
- En accedir a aquest lloc, els usuaris poden ser enganyats per descarregar un arxiu maliciós que després s'instal·la al seu dispositiu.
- El codi maliciós pot robar dades, bloquejar l'accés al sistema (programari de segrest) o fins i tot ser utilitzat per fer atacs de denegació de serveis (DDoS).

4.4. Anuncis maliciosos

El atacants fan servir *parking domains* per mostrar anuncis que poden ser enganyosos i contenir enllaços maliciosos que, en ser clicats, descarreguen codi maliciós o redirigeixen a altres llocs compromesos.

La manca de control i supervisió en algunes xarxes de publicitat més petites, que solen ser utilitzades pels serveis de *parking domains*, pot ser aprofitada pels atacants per dur a terme atacs de redirecció a pàgines malicioses o no desitjades. Això passa perquè aquestes xarxes publicitàries sovint tenen menys requisits de seguretat i un procés de verificació més laxa en comparació amb les grans plataformes publicitàries.

Com es fa això?

- L'atacant registra un *parking domain* i el vincula a aquestes xarxes publicitàries més petites. La manca de control en aquestes xarxes publicitàries les converteix en un vector ideal per als atacants que cerquen fer-hi activitats il·legals o perjudicials.

- En integrar anuncis en aquests llocs web fraudulents, els atacants aconsegueixen redirigir els visitants a pàgines de destinació malicioses. Com que no estan tan controlades com les xarxes publicitàries més grans, aquestes xarxes petites poden permetre que els atacants triïn de manera fàcil els *parking domains*, i n'injectin anuncis enganyosos o perillosos sense ser detectats ràpidament. Amb això es pot robar informació personal, propagar codi maliciós o, fins i tot, fer fraus publicitaris.

5. AUGE I PROBLEMÀTICA DELS *PARKING DOMAINS*

Tal com hem explicat, els *parking domains* són dominis registrats que no estan en ús actiu, i mostren moltes vegades una pàgina en blanc o anuncis automatitzats gestionats per plataformes, com ara Sedo, GoDaddy o Afternic. El seu ús ha augmentat perquè, com que no pugen un web, és difícil fer accions contra els atacants. Els són molt útils perquè és molt difícil aconseguir-ne el *takedown* o desmuntatge.

5.1 Augment dels *parking domains* per a finalitats malicioses

Tot i que aquesta informació correspon a l'any 2020, ens serveix per il·lustrar l'augment dels *parking domains* per a finalitats malicioses. Entre març i setembre de 2020, Palo Alto Networks va descobrir 5 milions de *parking domains* acabats d'«estacionar», o noms de domini registrats que estaven esperant ser utilitzats o activats. Sumat a això, 6 milions de dominis estacionats van canviar de categoria; el 31 % van esdevenir «sospitosos».

Algunes dades rellevants:

- Un 1 %, o 60.000, dels dominis estacionats van rebre l'etiqueta de «maliciosos», perquè hi incloïen activitats de pesca o codi maliciós. Cal destacar que els *parking domains* tenen vuit vegades més probabilitats de canviar d'una categoria benigna a una de perillosa.
- Gairebé un terç d'aquests *parking domains* «maliciosos» ho van fer en menys de 10 dies després de ser «estacionats». Per altra banda, els dominis benignes romanen estacionats entre 60 i 69 dies. Amb aquestes dades, Palo Alto conclou que els atacants no permeten que els seus dominis «envelleixin», cosa que ajuda a evitar-ne la detecció.

5.2 Dificultats per aconseguir el *takedown* dels *parking domains*

Demanar el *takedown* o desmuntatge d'un domini estacionat per raons de seguretat o protecció de marca és un procés complex.

5.2.1. Dificultats per aconseguir el *takedown* dels *parking domains*

- **Manca de contingut actiu**: atès que els parking domains no cometen violacions actives, no hi ha base legal per eliminar-los.

- **Els anuncis automatitzats no justifiquen una eliminació**: molts parking domains mostren anuncis, que són col·locats automàticament per plataformes publicitàries i no són controlats directament pel propietari del domini. A menys que un anunci específic estigui violant drets, la sola presència de publicitat automatitzada no justifica una eliminació.

5.2.2. *Takedown* de *parking domains* maliciosos

Les sol·licituds d'eliminació de dominis generalment requereixen la presència de contingut infractor com ara llocs web fraudulents, pàgines de pesca o material protegit per drets d'autor. Atès que els *parking domains* normalment no allotgen cap contingut actiu, no hi ha raons vàlides per sol·licitar-ne l'eliminació. Per aconseguir l'eliminació d'un *parking domain*, cal demostrar el següent:

- Ús no autoritzat d'una marca registrada.
- Allotjar-hi contingut il·legal o ofensiu.
- Frau, pesca o algun tipus d'engany premeditat.

En molts casos, per fer un *takedown* s'exigeix que s'identifiqui i demostri que al lloc web del qual s'ha informat es fa servir algun tipus de formulari per recopilar informació (correus, contrasenyes) de manera maliciosa. I, com en el cas dels *parking domains* que no es puja un web, això no es pot demostrar.

6. CONCLUSIONS I RECOMANACIONS

La suplantació de dominis, especialment a través de l'ús de *parking domains*, és una amenaça en evolució constant. És fonamental que tant les organitzacions com els consumidors siguin conscients dels perills inherents a aquests dominis maliciosos i adoptin pràctiques de seguretat proactives. En prendre les mesures pertinents i en estar informats sobre les tàctiques més recents que fan servir els atacants, és possible minimitzar l'èxit de possibles atacs.

En termes generals, les empreses han de fer un seguiment proper dels *parking domains* vinculats a aquestes i conscienciar sobre els riscos cibernètics. Per altra banda, els usuaris s'han d'assegurar d'escriure correctament els noms de domini i verificar que els propietaris del domini siguin confiables abans d'entrar en qualsevol lloc.

Tot seguit, presentem recomanacions més concretes tant per a empreses com per a usuaris.

6.1. Recomanacions per a empreses

- **Registre estratègic de dominis**: adquirir variacions del domini d'una empresa evita que tercers els registrin més endavant, per evitar que els atacants s'aprofitin del *typosquatting*.

- **Monitoratge dels *parking domains***: les empreses han de dur a terme un seguiment constant dels *parking domains* que puguin estar relacionats amb la seva marca o negoci. Fer servir eines de monitoratge de dominis pot ajudar a detectar qualsevol activitat sospitosa que pugui afectar la reputació de la marca i evitar atacs de suplantació.

- **Implementació d'estratègies de protecció de marca digital**: les empreses poden implementar solucions de protecció de marca en línia per rastrejar el possible ús indegut del seu nom.

- **Implementació de protocols de seguretat**: es recomana adoptar tecnologies que ajudin a prevenir la suplantació de dominis en correus electrònics. A més, habilitar l'autenticació de dos factors i mantenir els sistemes de seguretat actualitzats redueix el risc que els atacants aconsegueixin accedir a la informació delicada.

- **Col·laboració amb les xarxes publicitàries confiables**: és crucial que les empreses col·laborin tan sols amb les xarxes publicitàries que disposin de mecanismes de verificació i seguretat sòlids. Quan les xarxes publicitàries més petites no estan ben controlades, poden ser un blanc per als atacants.

- **Formació**: les empreses han d'invertir en la capacitació contínua dels equips dels diferents departaments per mantenir-los al corrent de les últimes tècniques dels atacants i les millors pràctiques per mitigar els riscos de la suplantació de dominis.

6.2. Recomanacions per a usuaris/consumidors

- **Verificació de noms de domini**: els usuaris han de ser especialment curosos en introduir les direccions de llocs web en els navegadors. Escriure correctament els noms de domini és

crucial per evitar caure en llocs web falsos. També és recomanable comprovar si el domini té un certificat SSL vàlid (representat per «https://») i comprovar que el lloc web és autèntic abans de fer qualsevol acció.

- **Desconfiança de les grans ofertes**: si un lloc web sembla sospitosament atractiu o presenta una oferta molt bona, els usuaris han de procedir amb precaució. Els atacants sovint fan servir llocs falsificats per atraure les víctimes amb promocions enganyoses. És important confirmar l'autenticitat del lloc mitjançant una cerca d'opinions o amb la verificació de la reputació de la pàgina.

- **Ús de les eines de seguretat**: els consumidors han d'instal·lar i mantenir actualitzats els programaris antivirus i de protecció contra la pesca informàtica. Moltes eines de seguretat alerten sobre els llocs web potencialment perillosos, cosa que ajuda a prevenir l'accés a les pàgines malicioses.

- **Educació sobre la pesca informàtica**: els consumidors han d'estar informats sobre els mètodes de pesca i com els atacants poden fer servir la suplantació de dominis per enganyar les persones. Estar alerta amb els correus electrònics, missatges o llocs web sospitosos redueix les probabilitats de caure en fraus.

7. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.