
This is the **published version** of the bachelor thesis:

Cirilo Llorca, Aina. *Anàlisi i simulació d'un atac de phishing amb tècnica ClickFix*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Enginyeria Informàtica)

This version is available at <https://ddd.uab.cat/record/334410>

under the terms of the  license.

Anàlisi i simulació d'un atac de phishing amb tècnica ClickFix

Aina Cirilo Llorca

Resum—Actualment, el phishing és un dels vectors d'atac més freqüents i efectius en l'àmbit de la ciberseguretat. Aquest tipus d'amenaça combina tècniques d'enginyeria social, orientades a la manipulació psicològica de les víctimes mitjançant la generació d'urgència o autoritat, amb tècniques informàtiques que permeten la suplantació d'identitat i la creació d'entorns fraudulents. En alguns casos, aquestes tècniques no només busquen la captura de credencials, sinó també induir la víctima a executar accions que permetin la instal·lació de malware en el seu dispositiu. En aquest treball es presenta una anàlisi experimental d'un atac de spear phishing que utilitza la tècnica coneguda com ClickFix, en què una pàgina web fraudulenta simula errors o mecanismes de verificació per persuadir l'usuari d'executar instruccions que comprometen el sistema. L'estudi es desenvolupa mitjançant la simulació d'un entorn controlat, amb l'objectiu d'observar el comportament de l'atac i les seves conseqüències sobre els sistemes afectats. Posteriorment, es realitza una anàlisi dels resultats obtinguts amb la finalitat de veure l'impacte real d'aquest tipus d'atac i avaluar el seu risc.

Paraules clau—Phishing, ClickFix, Ciberseguretat, Enginyeria Social, Mitre Att&ck, Anàlisi, Malware, Stop, Djvu, Xifrat, Windows, PowerShell, Simulació, Virtualització.

Abstract— Currently, phishing is one of the most frequent and effective attack vectors in the field of cybersecurity. This type of threat combines social engineering techniques aimed at the psychological manipulation of victims through the creation of urgency or authority, with computing techniques that enable spoofing and the creation of fraudulent environments. In some cases, these techniques do not only aim to capture credentials, but also to induce the victim to execute actions that allow the installation of malware on their device. This work presents an experimental analysis of a spear phishing attack that uses the technique known as ClickFix, in which a fraudulent web page simulates errors or verification mechanisms to persuade the user to execute instructions that compromise the system. The study is carried out by simulating a controlled environment, with the aim of observing the behavior of the attack and its consequences on the affected systems. Subsequently, an analysis of the results obtained is carried out in order to see the real impact of this type of attack and evaluate its risk.

Index Terms—Phishing, ClickFix, Cybersecurity, Social Engineering, Mitre Att&ck, Analysis, Malware, Stop, Djvu, Encryption, Windows, PowerShell, Simulation, Virtualization.



1. INTRODUCCIÓ - CONTEXT DEL TREBALL

Segons l'Informe de Ciberseguretat 2025 de INCIBE [3], a Espanya es van registrar 122.223 incidents de ciberseguretat, un 26% més que l'any anterior. D'aquests incidents, 25.133 (≈20%) van ser phishing i 55.411 (≈45%) estaven relacionats amb malware, la qual cosa mostra clarament que aquests tipus d'atacs continuen sent una de les principals amenaces tant per a individus com per empreses i entitats.

A partir d'aquest context, aquest treball es centra en l'anàlisi d'un atac amb vector d'entrada phishing, concretament amb la tècnica ClickFix, en què una pàgina web fraudulenta simula errors o mecanismes de verificació per persuadir l'usuari a executar accions que permeten introduir malware al seu sistema. L'objectiu és observar com es produeix la intrusió, quins efectes pot tenir sobre els sistemes

afectats i avaluar posteriorment les possibles repercussions d'aquest tipus d'atacs.

Aquest tipus d'atac pot ser especialment perillós perquè pot paraitzar operacions i generar grans pèrdues. Un exemple és MGM Resorts [5], un operador de diversos hotels i casinos del Strip de Las Vegas, com el Bellagio, l'Aria i el Cosmopolitan. Els atacants van aconseguir accedir inicialment mitjançant enginyeria social, utilitzant informació del perfil de LinkedIn d'un usuari sènior per restablir l'autenticació multifactor (MFA) a través del servei intern d'assistència. Un cop dins, van aconseguir persistència configurant un proveïdor d'identitat addicional a Okta, cosa que els va permetre controlar els sistemes de gestió d'identitats i els entorns en núvol de Microsoft Azure, amb privilegis d'administrador. Aquesta intrusió va paraitzar centenars de servidors, provocant que màquines escurabutxaques i sistemes de pagament deixessin de funcionar, les reserves es bloquegessin i els clients no poguessin facturar ni sortir ni entrar. Com a conseqüència, els hotels i casinos van haver de tancar temporalment durant 10 dies mentre

* E-mail de contacte: aina.cirilo@autonoma.cat
* Menció realitzada: Tecnologies de la Informació
* Treball tutoritzat per: Enric Alibech (Departament d'Enginyeria de la Informació i de les Comunicacions)
* Curs 2025/26

es resolia l'incident, generant pèrdues econòmiques superiors als 80 milions de dòlars i afectant també la reputació i la normalitat del servei.

En resum, aquest exemple mostra com el phishing com a vector d'entrada pot ser extremadament perillós. Una vegada els atacants aconseguixen enganyar la víctima i obtenir accés inicial, poden executar moviments laterals dins del sistema i desplegar altres tipus d'atacs, com el ransomware en empreses grans o el malware com el nostre estudi pràctic.

2. OBJECTIUS

2.1 Objectiu general (OG)

Dissenyar, implementar i analitzar una simulació controlada d'un atac de phishing amb tècnica ClickFix en un entorn de laboratori, amb l'objectiu de comprendre com aquest tipus d'atac pot afectar un sistema i estudiar les possibles conseqüències que pot generar.

2.2 Objectius específics (OE)

1. **Analitzar el funcionament del ClickFix:** comprendre com es desenvolupa un atac des del primer contacte amb la víctima fins a l'execució de malware, estudiant com s'utilitzen mecanismes d'enginyeria social per enganyar l'usuari. Aquest anàlisi es basa en el model de *MITRE ATT&CK* per identificar les diferents fases de l'atac i les tècniques implicades.
2. **Dissenyar i construir l'escenari d'atac:** crear un entorn simulat que permeti reproduir de manera controlada el procés d'infecció, incloent un correu electrònic fraudulent i una pàgina web amb tècnica ClickFix, amb la finalitat d'observar com una víctima pot ser induïda a executar accions comprometedores sense percebre el risc real.
3. **Executar l'atac ClickFix:** dur a terme l'execució de l'atac per analitzar el comportament complet de la cadena d'infecció, des del moment en què la víctima interactua amb el contingut fraudulent fins a l'execució del malware, observant com aquest compromet el sistema, quines accions realitza i quins recursos o fitxers es veuen afectats.
4. **Analitzar l'impacte:** avaluar l'impacte de l'atac des del punt de vista de la víctima, analitzant el nivell de compromís del sistema, la dificultat de detecció, les evidències generades i les possibles conseqüències de seguretat derivades d'aquest tipus d'intrusió.

3. METODOLOGIA

Aquest treball segueix una metodologia estructurada en diverses fases seqüencials, inspirada en el model en cascada:

Fase 1: Marc teòric del treball (16/02/2026-12/04/2026)

En aquesta fase inicial es realitza una revisió bibliogràfica per establir els fonaments teòrics del treball i definir l'atac.

Les principals activitats desenvolupades són:

- Cerca inicial sobre diferents tipus d'atacs de ciberseguretat i les seves característiques principals.
- Selecció de l'atac que serà analitzat en el projecte.
- Estudi del funcionament del phishing, les seves variants i les tècniques d'enginyeria social associades.
- Anàlisi específica de la tècnica ClickFix i les seves diferents etapes agafant de referència el model de *MITRE ATT&CK*.
- Definició del marc conceptual i de les bases teòriques del projecte.

Fase 2: Disseny de l'escenari d'atac (13/04/2026-03/05/2026)

En aquesta fase es dissenya l'entorn experimental que permetrà reproduir l'atac en un context controlat.

Les activitats principals són:

- Disseny d'un escenari amb dues màquines virtuals: una que representa la víctima i una altra l'atacant, per poder simular la interacció entre els dos.
- Creació del correu electrònic fraudulent, pensat per enganyar l'usuari i fer que accedeixi a un enllaç que el redirigeix a una pàgina web falsa.
- Desenvolupament de la pàgina web que imita una pàgina real i, per tant, sembla legítima, però que incorpora una trampa de tipus ClickFix. Aquesta trampa està dissenyada perquè la víctima acabi introduint el malware al sistema sense donar-se'n compte.
- Ajuntar tots els elements per construir un atac coherent i realista.

Fase 3: Simulació i execució de l'atac (04/05/2026-24/05/2026)

Un cop dissenyat l'escenari, s'executa l'atac en l'entorn controlat.

Durant aquesta fase es duen a terme les següents tasques:

- Enviament del correu de phishing i simulació de la seva recepció per part de la víctima.
- Simulació del moment en què la víctima cau a la trampa, accedeix a la pàgina fraudulenta i executa les instruccions indicades pel ClickFix.
- Introducció i execució del malware en el sistema.

- Observació del comportament del sistema durant el procés d'intrusió, identificant els canvis que es produeixen un cop el malware està actiu.

Fase 4: Recollida d'evidències (25/05/2026-07/06/2026)

En aquesta fase es recopilen les evidències que s'han trobat de l'atac des de l'ordinador de la víctima, per després poder analitzar-ho en profunditat.

Les principals accions realitzades són:

- Recollida d'evidències que indiquin que el sistema ha estat atacat.
- Anàlisi del comportament del malware, observant quines accions ha realitzat un cop executat i com ha afectat el funcionament del sistema.
- Identificació de les possibles perjudicis causades, tant a nivell de sistema com d'accés a informació o recursos.
- Documentació de totes les proves obtingudes durant l'atac, recollint els resultats per poder-los utilitzar en l'anàlisi posterior.

Fase 5: Anàlisi dels resultats (08/06/2026-21/06/2026)

En aquesta fase es realitza una anàlisi detallada de tota la informació recollida per entendre l'abast real de l'atac.

Les activitats realitzades són:

- Identificació del possible origen de l'atac, intentant determinar si es pot trobar informació sobre l'atacant.
- Avaluació del grau de compromís del sistema, analitzant fins a quin punt ha estat afectat i quins recursos o dades poden haver quedat exposats.
- Valoració de l'impacte de l'atac sobre la víctima, tant a nivell del sistema com de risc per a la seguretat.
- Extracció de conclusions a partir dels resultats obtinguts, amb l'objectiu d'entendre millor les conseqüències d'aquest tipus d'atacs i el seu risc real.

3.1 Evolució del treball

El projecte, que inicialment es plantejava com la reproducció d'una infraestructura empresarial completa amb servidors, bases de dades i múltiples vectors d'atac, ha acabat evolucionant cap a un estudi més focalitzat i controlat. La reducció de l'escenari a dues màquines virtuals i a un únic atac basat en ClickFix ha estat una decisió clau des del punt de vista metodològic, ja que ha permès aprofundir amb més detall en cada fase de l'atac i millorar la qualitat de l'anàlisi realitzada.

Pel que fa al malware, el plantejament original era fer l'atac de tipus d' HijackLoader amb Arechclient2. Tanmateix, la necessitat d'aïllar completament l'entorn d'Internet per

motius de seguretat va obligar a descartar aquesta opció, ja que aquest tipus d'atac depèn de comunicacions externes per completar el procés d'infecció. En el seu lloc, es va seleccionar una mostra de ransomware de la família STOP/Djvu, que pot operar de manera autònoma dins del mateix sistema sense requerir connexió a servidors externs.

Durant la primera execució de l'atac, es va produir un contratemps inesperat: les eines de monitoratge instal·lades prèviament a la màquina víctima van quedar xifrades pel ransomware abans de poder recollir cap dada. Aquest fet va obligar a replantejar completament l'enfocament analític i a adoptar una metodologia d'anàlisi forense basada en utilitats natives de Windows, sense dependència d'eines especialitzades externes. Lluny de ser un obstacle, aquesta situació va permetre reproduir un escenari molt més proper a la realitat d'una resposta a incidents, on no sempre es disposa dels recursos ideals i cal treballar amb el que el sistema ofereix.

Posteriorment, es va repetir l'execució de l'atac en un entorn preparat adequadament, amb monitoratge actiu des de l'inici, cosa que va permetre complementar l'anàlisi forense amb observació en temps real del comportament del malware.

4. ESTAT DE L'ART

L'atac analitzat en aquest treball segueix una estructura en cadena, on cada fase prepara la següent. Es tracta d'un atac de phishing basat en enginyeria social, en el qual s'utilitza la tècnica ClickFix per induir la víctima a executar codi maliciós de manera voluntària. Això provoca que sigui el mateix usuari qui inicia el procés d'infecció, permetent així el desplegament del malware destinat al control remot del sistema i a l'extracció d'informació.

La nostra víctima simula ser el tresorer d'una empresa i rep un correu del CEO demanant, amb certa urgència, que comprovi si s'han enviat correctament les nòmines dels treballadors des de l'entitat bancària, acompanyat d'un enllaç que el dirigeix a la pàgina web de la suposada entitat. Tanmateix, el correu no prové realment del CEO de l'organització i la pàgina web tampoc és l'original, sinó una còpia dissenyada per semblar legítima, on apareix un missatge d'error que forma part de l'engany.

Aquest missatge forma part de la tècnica ClickFix, una altra modalitat de l'enginyeria social, que es basa en fer creure a la víctima que hi ha hagut un problema perquè així, amb la intenció de solucionar-lo, segueixi les nostres instruccions i executi una comanda maliciosa al seu propi sistema, a través del quadre Executar de Windows.

Quan la víctima segueix aquestes indicacions i executa la comanda, s'inicia realment la infecció del sistema. Aquesta acció permet descarregar i executar codi maliciós utilitzant eines legítimes del propi sistema operatiu, fet que dificulta la seva detecció.

En aquest cas es desplega el ransomware STOP/Djvu, que té com a objectiu el xifrat dels fitxers del sistema de la víctima mitjançant tècniques de criptografia, bloquejant-ne així l'accés. Un cop actiu, el malware afecta principalment documents, imatges i altres dades personals, modificant els fitxers amb extensions específiques i generant una nota de rescat amb les instruccions per al pagament exigint pels atacants. En algunes variants, també pot intentar dificultar la recuperació de la informació eliminant còpies de seguretat o punts de restauració del sistema.

En conjunt, aquest atac destaca per la seva naturalesa progressiva i modular. Cada fase té un objectiu específic i contribueix a reduir la probabilitat de detecció mentre augmenta el nivell de compromís del sistema. Aquesta combinació d'enginyeria social i malware fa que sigui especialment efectiu i difícil de mitigar amb mesures de seguretat tradicionals.

5. ANÀLISI ESTÀTICA

5.1 Model MITRE ATT&CK

Per analitzar aquest atac des d'una perspectiva estructurada, s'utilitza el model MITRE ATT&CK [15], un marc de referència àmpliament utilitzat en ciberseguretat que permet descriure de manera organitzada les tàctiques i tècniques utilitzades pels atacants. Aquest model facilita la comprensió dels atacs com una seqüència de fases successives, des de les primeres etapes de compromís fins a l'impacte final sobre el sistema.

Segons aquest model, l'arquitectura del nostre atac ClickFix es pot representar com un flux amb les següents etapes, que seran desenvolupades en detall en els subapartats següents:

5.2 Accés Inicial – Phishing (T1566)

L'atac presentat en aquest treball comença a l'etapa Accés Inicial, on fa servir el concepte de Phishing.

El Phishing engloba diferents tàctiques, però totes es basen en una combinació d'enginyeria social i tècniques informàtiques.

La part de enginyeria social té com a objectiu enganyar les víctimes perquè revelin informació sensible, realitzin accions fraudulentament o executin programari maliciós en els seus dispositius. Per aconseguir-ho, els atacants acostumen a situar la víctima en un context que li resulta familiar i afegeixen un cert grau d'urgència perquè no tinguin temps de qüestionar si allò és real o no. Un exemple molt habitual són les estafes bancàries, on la víctima rep un SMS del seu banc (context familiar), informant d'un error (urgència)

demanant que introdueixi les dades de la targeta (revelació d'informació sensible) per solucionar el problema tant ràpid com sigui possible.

A diferència d'altres atacs que exploten vulnerabilitats tècniques del programari o de la infraestructura, el phishing es centra en el factor humà com a vector principal d'entrada.

Com s'ha mencionat anteriorment, també hi ha una part informàtica que reforça l'engany, com pot ser l'enviament de correus fraudulents o SMS (smishing), la suplantació de veu (vishing) o la creació de codis QR i pàgines web malicioses.

5.3 Execució - Execució de l'Usuari (T1204)

El ClickFix és una tècnica d'enginyeria social que es basa en simular un problema tècnic amb l'objectiu de manipular el comportament de la víctima i aconseguir l'execució de codi maliciós. A diferència d'altres mètodes d'infecció més automatitzats, aquesta tècnica requereix una participació activa de l'usuari. Habitualment, es mostren missatges que imiten errors del sistema, verificacions de seguretat per identificar robots (com CAPTCHAs) o incidències del navegador, induint la víctima a realitzar una acció necessària per poder continuar.

Aquests missatges inclouen instruccions detallades per resoldre el suposat problema, indicant a l'usuari que obri una consola del sistema, com ara PowerShell o la terminal, i que hi copiï una comanda proporcionada a la mateixa pàgina. En molts casos, aquestes comandes es presenten de manera ofuscada o codificada per ocultar la seva intenció real. Tot i que aparenten ser una solució a una incidència, en realitat permeten a l'atacant obtenir un primer accés al sistema i iniciar l'execució de codi maliciós.

Aquesta dependència de l'acció de l'usuari fa que, dins del model MITRE ATT&CK, aquest comportament es classifiqui dins de la tècnica Execució de l'Usuari, ja que és la pròpia víctima qui, de manera voluntària però enganyada, executa les instruccions malicioses.

Dins d'aquesta tècnica, es poden identificar diverses sub-tècniques rellevants. La primera s'anomena Còpia i Enganxa Maliciosa i consisteix, com bé diu el seu nom, a induir l'usuari a copiar i executar comandes malicioses provinents d'una font controlada per l'atacant, aparentment fiable, dins d'un interpret de comandes o scripts del sistema. Aquest enfocament és especialment efectiu perquè l'acció es realitza manualment i dins d'un entorn legítim, fet que pot permetre evitar mecanismes de protecció.

La segona és la tècnica de Fitxer Maliciós, que es basa en convèncer la víctima perquè obri o executi un fitxer amb l'objectiu de desencadenar l'execució de codi maliciós al sistema. Els fitxers utilitzats en aquest tipus d'atacs poden

presentar-se en formats habituals com documents, PDFs, fulls de càlcul o fitxers executables, entre d'altres. Per augmentar la probabilitat que la víctima els obri, els atacants utilitzen tècniques de disfressa (*masquerading*), fent que el fitxer sembli inofensiu o relacionat amb l'activitat habitual de l'usuari. A més, també poden aplicar tècniques d'ofuscació del contingut o protegir el fitxer amb contrasenya, acompanyant-lo d'instruccions específiques per facilitar-ne l'obertura i reforçar la seva credibilitat.

En conjunt, aquestes tècniques evidencien com l'atac utilitza el comportament de l'usuari com a vector principal d'execució, evitant mecanismes automàtics i dificultant la detecció per part de les solucions de seguretat tradicionals.

5.4 Execució – Intèrpret de comandes i scripts (T1059)

Aquesta fase consisteix en l'execució de comandes o scripts mitjançant intèrprets que ja estan inclosos al sistema operatiu. Això permet als atacants executar codi utilitzant eines del mateix sistema, sense necessitat d'afegir programes externs, fet que dificulta la seva detecció. Aquests intèrprets són eines normals del sistema i serveixen per automatitzar tasques, per això sovint poden semblar activitats habituals d'administració. A més, aquesta tècnica es pot utilitzar en diferents moments de l'atac, tant per iniciar l'execució com per descarregar fitxers, recollir informació o comunicar-se amb altres sistemes.

Dins d'aquesta tècnica, una de les sub-tècniques més rellevants és PowerShell (T1059.001). PowerShell és una interfície de línia de comandes i un entorn de scripting inclòs en sistemes Windows. Els atacants poden aprofitar aquesta eina per executar codi maliciós, descarregar contingut des d'Internet i executar-lo directament, fins i tot sense necessitat d'escriure fitxers al disc. A més, PowerShell permet executar comandes de forma local o remota, així com llançar altres processos o scripts, fet que el converteix en una eina molt versàtil dins d'una cadena d'atac.

5.5 Evasió de Defensa – Desofuscar/descodificar fitxers o informació (T1140)

En aquesta fase, els atacants utilitzen tècniques destinades a dificultar la detecció del codi maliciós mitjançant l'ús d'ofuscació. Aquest procés consisteix a ocultar el contingut maliciós durant la seva distribució o emmagatzematge, i posteriorment recuperar-ne la forma original abans de la seva execució. L'objectiu principal és evitar que eines de seguretat, com antivirus o sistemes de detecció, puguin identificar el codi maliciós en les fases inicials de l'atac.

Per aconseguir-ho, es poden utilitzar diferents mètodes d'ofuscació, com la codificació en Base64, l'ús d'algoritmes de xifrat o la fragmentació del codi en múltiples parts. En

el context d'aquest treball, aquesta tècnica s'aplica a les comandes que ha d'executar l'usuari, les quals poden estar codificades o ofuscades, fet que en dificulta la interpretació i la comprensió de la seva funcionalitat. Aquest procés pot realitzar-se mitjançant scripts o utilitats del sistema, com PowerShell, que permeten transformar dades codificades en codi executable.

Finalment, aquest procés de desofuscació pot produir-se en diferents moments de l'atac, tant immediatament després de la descàrrega del codi com en fases posteriors, un cop l'atacant ja ha establert presència al sistema. Aquest comportament és habitual en cadenes d'infecció complexes, on cada etapa permet desplegar la següent, dificultant així l'anàlisi del malware.

5.6 Impacte - Xifrat de dades (T1486)

Aquesta fase es basa en el bloqueig de l'accés a la informació del sistema compromès mitjançant el xifrat dels fitxers, amb la finalitat de generar un impacte directe sobre la disponibilitat de les dades.

Aquest comportament és propi dels atacs de ransomware, en què el codi maliciós identifica contingut rellevant dins del dispositiu i el codifica de manera que no pugui ser consultat ni utilitzat per la víctima. Un cop finalitzat el procés, els atacants acostumen a deixar missatges o notes de rescat amb indicacions sobre com intentar recuperar l'accés als arxius afectats.

L'objectiu principal d'aquesta tècnica és alterar el funcionament normal del sistema compromès i limitar l'accés de l'usuari a la seva informació.

6. ANÀLISI DINÀMICA

6.1 Entorn virtualitzat i disseny de l'atac

Per dur a terme la simulació de l'atac de forma segura i controlada, s'ha utilitzat un entorn virtualitzat compost per dues màquines virtuals: una que simula l'ordinador de l'atacant i una altra que representa la víctima. Aquesta aproximació permet encapsular completament l'escenari d'atac, evitant que el malware pugui afectar el sistema host (ordinador personal) i garantint així un entorn aïllat per a l'experimentació.

A més, la virtualització permet reproduir un escenari molt proper a un entorn real, ja que cada màquina virtual disposa dels seus propis recursos virtualitzats (CPU, memòria RAM, emmagatzematge i interfícies de xarxa), així com d'un sistema operatiu independent.

Per a la creació i gestió de les màquines virtuals s'ha utilitzat VirtualBox, una eina de virtualització de codi obert àmpliament utilitzada en entorns acadèmics i professionals. VirtualBox permet executar múltiples sistemes operatius sobre un mateix sistema host, i en aquest cas hem fet servir dos sistemes diferents:

- **Víctima:** S'ha utilitzat una imatge de disc de Windows 11, ja que els atacs basats en la tècnica ClickFix estan principalment orientats a aquest sistema operatiu, especialment per l'ús d'eines com PowerShell i altres components nadius de Windows.
- **Atacant:** S'ha utilitzat Kali Linux, una distribució especialitzada en ciberseguretat basada en Linux. Aquest sistema operatiu inclou un ampli conjunt d'eines preinstal·lades per a la realització de proves de penetració, anàlisi forense i avaluació de vulnerabilitats.

El disseny de l'atac s'ha estructurat en dues fases. En una primera fase, centrada en l'enginyeria social, s'han creat comptes de Gmail específics per simular l'enviament de correus fraudulents, així com un correu enganyós destinat a reproduir el vector inicial de l'atac. Paral·lelament, s'ha desenvolupat una pàgina web falsa que reproduïx únicament el missatge d'error i les instruccions associades, amb l'objectiu de simular el comportament real d'un atac ClickFix. Aquesta pàgina s'ha dissenyat introduint petites variacions i errors ortogràfics intencionats per ajudar a diferenciar el contingut legítim del que seria una suplantació completa. Aquest detall és rellevant, ja que en un atac real no és habitual poder clonar exactament dominis o serveis legítims, atès que les URL i els continguts originals són únics.

En una segona fase, corresponent a l'execució del malware, s'ha configurat l'entorn per permetre la reproducció controlada del seu comportament. En primer lloc, s'ha desactivat completament l'accés a Internet amb l'objectiu d'evitar qualsevol comunicació externa del codi maliciós, garantint així que no es produís cap sortida de dades ni interacció amb sistemes reals. A continuació, s'ha establert una xarxa interna entre les màquines virtuals per permetre la comunicació entre l'atacant i la víctima dins d'un entorn completament aïllat.

Un cop definida la infraestructura de xarxa, s'ha introduït el programari maliciós i s'ha preparat per a la seva execució. Finalment, s'han desactivat les solucions de seguretat de Microsoft habilitades per defecte al sistema per evitar bloquejos durant la simulació i permetre l'execució completa del malware.

Pel que fa al codi maliciós utilitzat en la simulació, no s'ha desenvolupat codi maliciós propi, sinó que s'ha optat per utilitzar una mostra real obtinguda de la plataforma MalwareBazaar. Aquesta és una plataforma pública creada

per l'equip de Abuse.ch i té com a objectiu facilitar l'intercanvi i l'anàlisi de mostres de programari maliciós entre investigadors i professionals de la ciberseguretat. Disposa d'una extensa base de dades de mostres classificades segons tipus, signatures i etiquetes, cosa que permet seleccionar mostres representatives per a diferents escenaris d'atac.

En aquest cas, i tenint en compte que la simulació s'ha fet en un entorn totalment controlat amb l'accés a Internet desactivat per motius de seguretat, s'ha triat una mostra de ransomware STOP/Djvu. Aquesta decisió s'ha pres perquè es necessitava un tipus de malware que pogués funcionar de manera completa dins del mateix ordinador, sense dependre de connexions externes. Aquest ransomware permet xifrar els fitxers del sistema i pot fer-ho utilitzant diferents mecanismes de generació de claus, ja sigui en línia o, si no és possible, amb claus generades localment.

6.2 Anàlisi i recollida d'evidències

L'anàlisi s'ha dut a terme des de la perspectiva de la víctima amb l'objectiu de reconstruir el comportament del malware i les seves accions dins del sistema. L'estudi combina monitoratge actiu durant l'execució i anàlisi forense a posteriori.

6.2.1 Identificació inicial de l'atac

Un cop finalitzada la infecció, el sistema presentava tots els fitxers personals i executables amb l'extensió .gazp, i a l'escriptori s'havia generat una nota de rescat anomenada *_readme.txt*. Aquest document, visible a la Figura A.1, confirma la naturalesa de l'atac com a ransomware, detallant un sistema de xifratge amb clau única, un ID personalitzat de la víctima i les instruccions de pagament per a la recuperació de les dades.

6.2.2 Visor d'Esdeveniments

El Visor d'Esdeveniments recull automàticament tot el que passa al sistema. Revisant els registres de la franja horària de l'atac, el resultat més destacable és la falta total d'alertes: ni errors ni avisos en el moment de la infecció. El sistema no va detectar res sospitosos mentre l'atac tenia lloc.

L'única pista concloent apareix a la secció de Sistema, on hi ha una única evidència que indica que s'han actualitzat tres claus del registre i s'ha creat una pàgina modificada just un minut després de l'inici de l'atac. Aquest canvi encapta amb el comportament típic d'un ransomware que altera el sistema mentre xifra els fitxers.

6.2.3 Comunicacions de xarxa

Mitjançant la captura de tràfic amb Wireshark durant l'atac, s'ha pogut reconstruir la seqüència completa de la comunicació entre la màquina víctima (192.168.0.22) i la

màquina atacant (192.168.0.20) a través del port 8080. S’han identificat connexions TCP des de ports dinàmics de la víctima cap al servidor, acompanyades de paquets Keep-Alive que mantenen la sessió oberta durant el procés d’infecció. També s’han observat paquets SSDP (Simple Service Discovery Protocol) cap a l’adreça multicast 239.255.255.250, compatibles amb una fase d’exploració de la xarxa local.

L’evidència més rellevant es troba en el tancament formal de la connexió, on es visualitzen els paquets FIN/ACK entre les IPs mencionades i el detall de conversa marcada com a “Complete, WITH_DATA (31)” (Figura A.2). Això confirma que durant la sessió es va transferir contingut real, corresponent al lliurament del codi maliciós.

Un aspecte a destacar de l’anàlisi de xarxa és l’absència total de tràfic cap a adreces externes (fora de la xarxa 192.168.0.0/24). No s’han detectat consultes DNS a servidors externs ni intents de connexió TCP SYN cap a Internet, la qual cosa demostra que, en aquest entorn aïllat, el malware no va intentar establir comunicació amb cap servidor de C2 (Command & Control) ni realitzar exfiltració de dades.

6.2.4 Absència de persistència i elusió de la detecció

Una part rellevant de l’anàlisi és l’absència d’evidències persistents al sistema. Amb la Sysinternals Suite es va comprovar que Process Explorer no mostrava cap procés sospitós, ja que tots els processos en execució eren legítims de Microsoft. Aquest comportament mostra que, un cop finalitzat el procés de xifrat, el malware finalitza la seva execució i desapareix del sistema sense mantenir cap procés actiu.

De la mateixa manera, Autoruns no va detectar cap mecanisme de persistència, ni en claus de registre ni en serveis, tasques programades o extensions del sistema.

Pel que fa a l’anàlisi estàtica, els intents d’inspeccionar svc.exe amb PESTudio van fallar repetidament a causa del tancament inesperat de l’eina, probablement provocat per l’ofuscació o xifrat intern de l’executable.

6.2.5 Rastres al sistema de fitxers i execució

Com a anàlisi post-atac, s’ha utilitzat PowerShell per identificar fitxers creats o modificats durant la franja horària de l’atac. La cerca ha revelat indicis d’execució de programari nou al sistema, així com la presència de components temporals a les zones on Windows emmagatzema dades de sessió i treball de les aplicacions. Entre aquests rastres, destaca especialment la confirmació que PowerShell es va executar de forma automatitzada i no per acció manual de l’usuari, fet que indica que, un cop iniciat per la víctima, el procés d’infecció va continuar executant-se de manera autònoma.

L’evidència principal apareix a la carpeta temporal del sistema (AppData\Local\Temp): on es detecten quatre fitxers creats durant la franja temporal de l’atac. Es tracta de l’executable svc.exe, amb un nom que imita un servei legítim de Windows, i tres fitxers .tmp amb noms aleatoris UUID (identificadors únics). Aquest tipus de noms resulta sospitós perquè dificulta identificar-ne fàcilment l’origen i és habitual en malware que intenta passar desapercebut dins del sistema. La presència conjunta d’aquests fitxers confirma el desplegament del ransomware (Figura A.3). Per identificar-lo es va calcular el seu hash SHA256 i es va consultar a VirusTotal [26], una plataforma que permet analitzar fitxers sospitosos comparant-los amb bases de dades i motors antivirus de múltiples proveïdors. Aquesta consulta va confirmar que el fitxer corresponia al ransomware STOP/DJVU (Figura A.4).

Finalment, l’historial de comandes de PowerShell no conté la comanda maliciosa executada per la víctima. Això demostra que el malware va ser executat com a procés fill no interactiu, evitant així quedar guardat a l’historial de PowerShell.

6.2.6 Resultat de les eines de seguretat

Per completar la visió de l’evasió, s’han executat dues eines d’escaneig a posteriori. Fortect ha retornat que no s’havia detectat cap element en seguretat, i el Windows Security natiu del sistema operatiu, tampoc ha identificat cap amenaça (Figura A.5). El fet que fins i tot l’antivirus natiu, amb accés privilegiat al sistema, sigui incapaç de detectar rastres actius reforça la conclusió que, un cop el ransomware ha completat el xifrat i s’ha autoeliminat, no queda cap component maliciós actiu sobre el qual les eines de detecció puguin actuar.

7. AVALUACIÓ DEL RISC MITJANÇANT EL MODEL DREAD

Per quantificar el risc de l’atac analitzat s’ha aplicat el model DREAD de Microsoft, un marc d’avaluació d’amenaçes que puntua cada risc en cinc dimensions de l’1 al 10. La puntuació final s’obté calculant la mitjana de les cinc categories.

Criteri	Puntuació
Damage (Dany)	10
Reproducibility (Reproductibilitat)	10
Exploitability (Explotabilitat)	10
Affected Users (Usuaris afectats)	2.5
Discoverability (Detectabilitat)	8
Total:	8.1

Justificació:

- Danys: Tots els fitxers personals i executables han quedat xifrats i inaccessibles, el sistema ha perdut funcionalitat parcial i les dades no es poden recuperar sense la clau.
- Reproductibilitat: L'atac és molt fàcil de reproduir, només requereix un correu de phishing i una pàgina web fraudulenta amb la tècnica ClickFix.
- Explotabilitat: L'única acció necessària és que la víctima copii i enganxi una comanda al seu propi sistema. No es requereix cap vulnerabilitat tècnica, ni accés previ al sistema, ni eines especialitzades per part de l'atacant. L'explotació s'executa des del propi navegador web de la víctima.
- Usuaris afectats: Com l'atac ha estat un *spear phishing* només ha afectat a un sol usuari.
- Detectabilitat: La tècnica ClickFix ja està documentada en el domini públic (reportada per Microsoft, ESET i altres). Tot i això, la detecció activa durant l'atac és molt difícil, ja que el malware no genera alertes visibles ni deixa rastres persistents al sistema.

La puntuació de 8.1 sobre 10 situa aquest atac en la categoria de risc alt. On destaca especialment és en el dany causat: tots els fitxers del sistema queden inutilitzables de forma immediata, tot i que un cop el malware desapareix, els fitxers introduïts posteriorment no es veuran afectats.

La combinació de ClickFix i STOP/DJVU és fàcilment reproducible i escalable: tot i que en aquest treball s'ha simulat com a spear phishing individual, la mateixa tècnica podria arribar a moltes més víctimes si s'aconsegueix dirigir tràfic massiu a la pàgina fraudulenta.

Finalment, tot i que la tècnica està documentada públicament, l'anàlisi ha demostrat que és molt difícil de detectar en execució. Això reforça que la principal defensa és la conscienciació prèvia, ja que un cop executat l'atac no hi ha manera de revertir el dany causat.

8. RESULTATS

La simulació realitzada ha permès reproduir de manera controlada una cadena d'atac composta per diferents fases que en conjunt formen un únic procés d'infecció, des del primer contacte amb la víctima fins al compromís total del sistema.

La fase d'enginyeria social ha reproduït correctament el vector d'entrada de l'atac. La víctima, en rebre un correu aparentment legítim i accedir a la pàgina web fraudulenta, ha executat voluntàriament la comanda maliciosa sense

percebre cap risc. Aquesta acció ha estat el detonant de tota la cadena i és especialment significativa perquè no ha requerit cap vulnerabilitat tècnica del sistema.

Durant l'execució del malware, el sistema ha continuat funcionant amb aparent normalitat, sense generar cap alerta ni notificació de seguretat. Les captures de Wireshark han permès reconstruir el flux de comunicacions, confirmant la connexió TCP activa amb el servidor ClickFix durant la descàrrega del codi maliciós i l'absència total de tràfic cap a servidors externs. Un cop finalitzat el xifrat, el malware ha desaparegut del sistema sense deixar cap procés actiu ni mecanisme de persistència, tal com han confirmat Process Explorer i Autoruns.

Pel que fa a l'impacte, tots els fitxers personals i executables han quedat xifrats amb extensió .gasp i inaccessibles, acompanyats d'una nota de rescat. L'anàlisi forense posterior ha localitzat l'executable maliciós svc.exe a la carpeta Temp, creat exactament en el moment de l'atac, i la seva identitat ha estat confirmada com a STOP/DJVU mitjançant la consulta del hash SHA256 a VirusTotal. Tot i aquestes evidències, cap eina d'escaneig executada a posteriori ha estat capaç de detectar cap amenaça activa, evidenciant les limitacions de la detecció reactiva davant d'un ransomware que no deixa cap component actiu un cop ha completat la seva tasca.

En conjunt, els resultats obtinguts documenten una cadena d'atac completa i efectiva, on cada fase ha deixat evidències concretes que permeten reconstruir el procés d'infecció, tot i que cap eina de seguretat executada a posteriori ha estat capaç de detectar-la. L'avaluació del risc mitjançant el model DREAD ha obtingut una puntuació de 8,1 sobre 10, reflectint un impacte alt derivat principalment del dany immediat sobre el sistema i de la baixa dificultat d'execució per part de l'atacant.

9. CONCLUSIONS

Els objectius plantejats a l'inici del treball s'han assolit de manera satisfactòria. S'ha analitzat el funcionament de la tècnica ClickFix des d'una perspectiva estructurada, utilitzant el model MITRE ATT&CK com a marc de referència; s'ha dissenyat i construït un escenari d'atac funcional, compost per un correu de phishing i una pàgina web fraudulenta amb trampa ClickFix; s'ha executat l'atac de manera controlada, observant la cadena completa d'infecció des del primer contacte amb la víctima fins al compromís total del sistema; i finalment s'ha analitzat l'impacte real de l'atac, avaluant el nivell de compromís, les evidències generades i la dificultat de detecció.

Tot i així, a mesura que avançava el treball es van trobar algunes limitacions. La principal va ser la necessitat d'aïllar l'entorn d'Internet per motius de seguretat, decisió imprescindible per evitar qualsevol comunicació real del malware

amb sistemes externs, però que ha limitat l'observació de possibles comportaments del ransomware en condicions reals de connectivitat, com ara la comunicació amb servidors de Command & Control o la generació de claus de xifrat en línia. De la mateixa manera, no s'ha pogut elaborar una taula d'Indicadors de Compromís (IoCs) com estava previst inicialment, ja que la manca d'informació disponible sobre l'origen i la infraestructura de l'atacant ho ha impedit. Aquesta limitació s'ha resolt substituint-la per una avaluació de risc mitjançant el model DREAD, que permet quantificar el nivell de compromís del sistema de manera alternativa.

Encara que el treball no ha seguit el camí inicialment previst, els resultats obtinguts han estat igual de valuosos. Els contratemps viscuts durant el procés han aportat un aprenentatge que va més enllà del que hauria ofert un escenari perfectament controlat des del primer moment: gestionar aquests imprevistos ha obligat a estar alerta davant de qualsevol acció que pogués comprometre l'ordinador amfitrió o fer malbé el laboratori sencer amb un pas en fals, i ha permès entendre de primera mà com actuen els atacants, quins vectors d'entrada utilitzen, quines tècniques i tàctiques despleguen i quines conseqüències reals pot tenir un atac d'aquestes característiques sobre un sistema.

Com a línia de treball futura, s'ha identificat l'estudi de mecanismes de mitigació i resposta a aquest tipus d'atacs, tant des del punt de vista preventiu com reactiu, aspecte que queda fora de l'abast del present treball.

Amb l'anàlisi d'aquest atac es pot concloure que, tot i que el ransomware representa la part més destructiva del procés, el punt més crític és l'enginyeria social. Aquestes tècniques no depenen de cap fallada tècnica del sistema, sinó del comportament de les persones, fet que les fa molt més difícils de prevenir.

Les estafes basades en l'engany no són un fenomen nou, però la tecnologia n'amplifica enormement l'abast i la velocitat. A més, quan apareix una variant que funciona, s'estén ràpidament entre els criminals abans que la societat en sigui plenament conscient o que existeixin defenses efectives.

No hi ha una solució definitiva per a aquest tipus d'atacs. Mesures més restrictives podrien limitar-los, però a costa de fer els sistemes menys funcionals i pràctics. Per aquest motiu, la millor defensa continua sent la combinació de conscienciació, bones pràctiques i eines de seguretat que s'adaptin constantment.

10. ÚS DE LA INTEL·LIGÈNCIA ARTIFICIAL

En el desenvolupament d'aquest treball s'ha fet ús d'eines d'intel·ligència artificial com a suport complementari en diferents fases del procés.

Concretament, s'ha utilitzat ChatGPT per a la millora de la redacció del document, facilitant la reformulació de textos, la correcció lingüística i l'estructuració d'idees. Així mateix, aquesta eina també s'ha utilitzat com a suport en el desenvolupament de la pàgina web utilitzada en la simulació de l'atac.

De manera complementària, s'ha utilitzat Claude per a l'anàlisi del codi de les mostres obtingudes de MalwareBazaar, així com per donar suport en la comprensió del seu comportament.

Tant ChatGPT com Claude també han estat utilitzats de forma conjunta per a la resolució d'errors, la depuració de codi i la configuració dels diferents components del projecte.

D'altra banda, s'ha fet servir Google Gemini per a la creació i modificació d'imatges utilitzades en la pàgina web de la simulació.

BIBLIOGRAFIA

- [1] M. Kosinski. "¿Qué es el phishing? | IBM". IBM [En línia]. Disponible: <https://www.ibm.com/es-es/think/topics/phishing>
- [2] "19 tipos de ataques de phishing con ejemplos | Fortinet". Fortinet. [En línia]. Disponible: <https://www.fortinet.com/lat/resources/cyberglossary/types-of-phishing-attacks>
- [3] incibe, "BalanceCiberseguridad2025_INCIBE.pdf", 9 de febrero de 2026, BALANCE DE CIBERSEGURIDAD 2025, https://www.incibe.es/sites/default/files/2026-02/Balance%20de%20ciberseguridad%202025%20INCIBE/BalanceCiberseguridad2025_INCIBE.pdf.
- [4] "Ciberataque a MGM Resorts: de la nube al casino - Skyhigh Security". Skyhigh Security. [En línia]. Disponible: <https://www.skyhighsecurity.com/es/about/resources/intelligence-digest/mgm-resorts-cyberattack-from-cloud-to-casino-floor.html>
- [5] Yegonnet. "MGM Resorts reanuda plenamente las operaciones de sus casinos y hoteles 10 días después de sufrir un ciberataque | Yegonnet Latinoamérica". Yegonnet | Latest casino, gambling and sports betting news. [En línia]. Disponible: <https://www.yegonnet.com/latinoamerica/noticias/2023/09/22/96234-mgm-resorts-reanuda-plenamente-las-operaciones-de-sus-casinos-y-hoteles-10-dias-despues-de-sufrir-un-ciberataque>
- [6] "Qué es ClickFix, una técnica de ingeniería social muy utilizada para distribuir malware". Award-winning news, views, and insight from the ESET security community. [En línia]. Disponible: <https://www.welivesecurity.com/es/ciberdelitos/que-es-clickfix-falsa-notificacion-instala-malware/>
- [7] John Hammond. *hackers trick everyone to run malware (FileFix)*. (1 de julio de 2025). [Video en línea]. Disponible: https://www.youtube.com/watch?v=Vz2ak0YW_L4

[8] Enderman. *What happens if you click a fake CAPTCHA?* (5 de agosto de 2025). Disponible: <https://www.youtube.com/watch?v=bQMOLVbRfGE>

[9] "Think before you Click(Fix): Analyzing the ClickFix social engineering technique | Microsoft Security Blog". Microsoft Security Blog. [En línea]. Disponible: <https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/>

[10] S. Bitam. "Un cliente desastroso: del engaño de ClickFix al robo de información — Elastic Security Labs". Elastic — The Search AI Company | Elastic. [En línea]. Disponible: <https://www.elastic.co/es/security-labs/a-wretch-client>

[11] "ClickFix Gets Creative: Malware Buried in Images | Huntress". Huntress. Disponible: <https://www.huntress.com/blog/clickfix-malware-buried-in-images>

[12] Shrutirupa Banerjee. "Desmontando un engaño cibernético: un análisis de la campaña de phishing Clickfix HijackLoader". Blogs on Information Technology, Network & Cybersecurity | Seqrite. Disponible: <https://www.seqrite.com/es/blog/deconstructing-a-cyber-deception-an-analysis-of-the-clickfix-hijackloader-phishing-campaign/>

[13] "Intelligence Insights: HijackLoader, Arechclient2, and Amber Albatross". Red Canary. Disponible: <https://redcanary.com/blog/threat-intelligence/intelligence-insights-april-2025/>

[14] "MalwareBazaar | Checking your browser". MalwareBazaar | Malware sample exchange. [En línea]. Disponible: <https://bazaar.abuse.ch/browse.php?search=tag:hijackload>

[15] "MITRE ATT&CK®". MITRE ATT&CK®. [En línea]. Disponible: <https://attack.mitre.org/>

[16] "Cyber Kill Chain®". Lockheed Martin. [En línea]. Disponible: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

[17] "Cómo hacer un análisis forense informático paso a paso". Berna Network -Tu partner tecnológico. Desarrollo y consultoría. [En línea]. Disponible: <https://www.bernanetwork.com/analisis-forense-informatico>

[18] "Explorador de procesos - Sysinternals". Microsoft Learn: Build with answers in reach. [En línea]. Disponible: <https://learn.microsoft.com/es-es/sysinternals/downloads/process-explorer>

[19] "Autoruns - Sysinternals". Microsoft Learn: Build with answers in reach. [En línea]. Disponible: <https://learn.microsoft.com/es-es/sysinternals/downloads/autoruns>

[20] "netstat". Microsoft Learn: Build with answers in reach. [En línea]. Disponible: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>

[21] Y. Fernández. "VirtualBox: qué es y cómo usarlo para crear una máquina virtual con Windows u otro sistema operativo". Xataka -

Tecnología y gadgets, móviles, informática, electrónica. Disponible: <https://www.xataka.com/basics/virtualbox-que-como-usarlo-para-crear-maquina-virtual-windows-u-otro-sistema-operativo>

[22] "¿Qué es Kali Linux y para qué se utiliza? | Blog de Arsys". Arsys. [En línea]. Disponible: [https://www.arsys.es/blog/que-es-kali-linux-y-para-que-se-utiliza?itc=ULIY4GX4-5ICVBT-W96AAJS&gad_source=1&gad_campaignid=23577242876&gad_gbrad=0AAAAAD-9fk8H9bMymu-5F\[Khp4fSaEyTO&gadclid=CjwKCAjwhe3OBhA-BEiwA6392zIsOt5brl-CkMV5nvjSxcp8nABV7bff-pbgZc1Is03O1eQhOWqOTpBoC86QQAxD_BwE](https://www.arsys.es/blog/que-es-kali-linux-y-para-que-se-utiliza?itc=ULIY4GX4-5ICVBT-W96AAJS&gad_source=1&gad_campaignid=23577242876&gad_gbrad=0AAAAAD-9fk8H9bMymu-5F[Khp4fSaEyTO&gadclid=CjwKCAjwhe3OBhA-BEiwA6392zIsOt5brl-CkMV5nvjSxcp8nABV7bff-pbgZc1Is03O1eQhOWqOTpBoC86QQAxD_BwE)

[23] S. D. Luz. "Cómo configurar las opciones de red de VirtualBox para las VMs". RedesZone. [En línea]. Disponible: <https://www.redeszone.net/tutoriales/redes-cable/configuracion-red-maquina-virtual-virtualbox/>

[24] CiberWiki. "Stop Ransomware". CiberWik. [En línea]. Disponible: https://darfe.es/ciberwiki/index.php?title=Stop_Ransomware

[25] incibe, "VirusTotal". [En línea]. Disponible: <https://www.incibe.es/ciudadania/herramientas/virus-total>

[26] "VirusTotal". VirusTotal. [En línea]. Disponible: <https://www.virustotal.com/gui/file/1bb689e95fd5ed5f70fd3ac60cf28d7aace52fea6b1ba00a257e19cbf50a71d/community>

[27] "Modelado de amenazas para conductores - Windows drivers". Microsoft Learn: Build with answers in reach. Accedido el 11 de junio de 2026. [En línea]. Disponible: <https://learn.microsoft.com/es-es/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers>

[28] "Threat Modeling with Microsoft DREAD - Satori". Satori. Accedido el 11 de junio de 2026. [En línea]. Disponible: <https://satori-cyber.com/glossary/threat-modeling-with-microsoft-dread/>

APÈNDIX

A: EVIDÈNCIES DE L'ANÀLISI DINÀMIC

ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you. This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
<https://we.tl/t-ZyZya4Vb8D>
Price of private key and decrypt software is \$980.
Discount 50% available if you contact us first 72 hours, that's price for you is \$490.
Please note that you'll never restore your data without payment.
check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:
support@freshmail.top

Reserve e-mail address to contact us:
datastorehelp@airmail.cc

Your personal ID:
074110sieidjLJVXs65t0hiY0Usr4A1G0xEwvvs9JcZKN0t1

Activar Windows
Ve a Configuración para Windows.

Figura A.4: Hash de l'executable svc.exe

Windows Security

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 6/10/2026 11:31 PM (quick scan)
0 threat(s) found.
Scan lasted 56 seconds
12672 files scanned.

Quick scan

Scan options

Allowed threats

Protection history

Figura A.5: Windows Security

Capturing from Ethernet

Time	Source	Destination	Protocol	Length	Info
9.3449.0863678	PCSSystemtec_31:2d:bc	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.22
0.3449.4420138	192.168.0.22	192.168.0.20	TCP	54	52551 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=652
1.3449.4421100	192.168.0.22	192.168.0.20	TCP	54	60331 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=652
2.3449.4426980	192.168.0.20	192.168.0.22	TCP	60	8080 → 52551 [FIN, ACK] Seq=1 Ack=2 Win=642
3.3449.4427624	192.168.0.22	192.168.0.20	TCP	54	52551 → 8080 [ACK] Seq=2 Ack=2 Win=65280 Le
4.3449.4430872	192.168.0.20	192.168.0.22	TCP	60	8080 → 60331 [FIN, ACK] Seq=1 Ack=2 Win=642
5.3449.4430889	192.168.0.22	192.168.0.20	TCP	54	60331 → 8080 [ACK] Seq=2 Ack=2 Win=65280 Le
6.3450.3283629	PCSSystemtec_31:2d:bc	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.22
7.3451.0870713	PCSSystemtec_31:2d:bc	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.22
8.3452.0840803	PCSSystemtec_31:2d:bc	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.22
9.3453.4996528	PCSSystemtec_31:2d:bc	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.22
0.3454.0778338	PCSSystemtec_31:2d:bc	PCSSystemtec_26:45:bc	ARP	42	Who has 192.168.0.20? Tell 192.168.0.22

> Frame 5050: Packet, 54 bytes on wire (432 bits), 54 bytes captured on interface 0
> Ethernet II, Src: PCSSystemtec_31:2d:bc (08:00:27:31:2d:bc), Dst: 08:00:27:31:2d:bc (08:00:27:31:2d:bc)
> Internet Protocol Version 4, Src: 192.168.0.22, Dst: 192.168.0.20
> Transmission Control Protocol, Src Port: 52551, Dst Port: 8080
 Source Port: 52551
 Destination Port: 8080
 [Stream index: 23]
 [Stream Packet Number: 70]
 > [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)

Figura A.2: Paquets TCP FIN/ACK que confirmen el tancament de la sessió

Directorio: C:\Users\victimaw\AppData\Local\Temp

Mode	LastWriteTime	Length	Name
-a----	5/21/2026 6:48 PM	0	3121ddb3-0e32-41ac-9830-046956ce0165.tmp
-a----	5/21/2026 6:48 PM	0	551df02e-ef47-4549-ad62-758f1d72cddc.tmp
-a----	5/21/2026 6:48 PM	0	c7d1c3ce-857a-42f2-8952-932ddeb8d519.tmp
-a----	5/21/2026 6:48 PM	756736	svc.exe

Figura A.3: Executable svc.exe i fitxers temporals a AppData\Local\Temp