ANDORRA DIGITAL

ANC.AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

GHOSTCALL

Abril 2026
Document d'ús públic

1. *GHOSTCALL*

GhostCaii

- Campanya d'enginyeria social que envia **invitacions falses a reunions** per executar programari maliciós o iniciar intrusions.
- Va adreçada a organitzacions tecnològiques, Web3 i de criptomonedes a Europa, Àsia, Índia, Turquia i Austràlia.
- Forma part d'operacions més àmplies del grup BlueNoroff/Lazarus, conegut pels atacs financers avançats.

No es tracta d'**una pesca tradicional**, sinó d'un abús de plataformes de confiança.

2. COM HO FAN?

La campanya **GhostCall** és un **ATAC D'ENGINYERIA SOCIAL ELABORAT**.

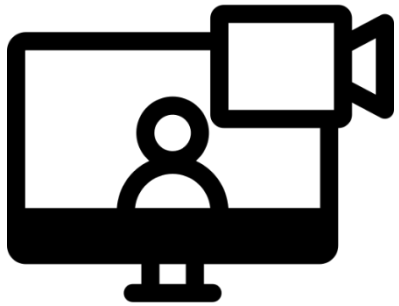
1

Suplantació d'identitat

Inversors de capital de risc, comptes compromesos d'empresaris, fundadors d'empreses emergents, etc.

2

Contacten amb les víctimes via Telegram



Les dirigeixen a reunions falses a través de **Zoom** o **Microsoft Teams**

3

Els indiquen que hi ha un **problema d'àudio**

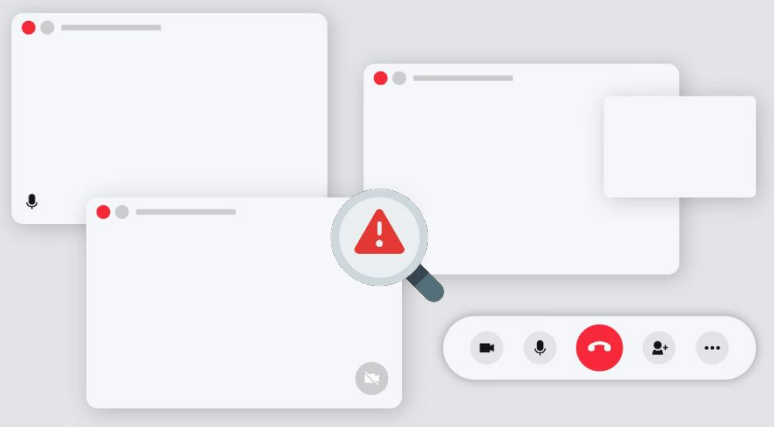
Sol·liciten **actualització**

Descarrega script maliciós que infecta l'equip

3. COM FUNCIONA EL *GHOSTCALL*

Com funciona l'atac?

El GhostCall combina enginyeria social amb tècniques d'intrusió molt sofisticades.



- **Invitació falsa a una reunió**: correu o missatge convincent que simula una reunió legítima a Zoom o Teams.
- **Enllaç maliciós**: l'enllaç porta a una pàgina que descarrega programari maliciós per a macOS.
- **Execució del programari maliciós**: el programari maliciós permet als atacants prendre el control del dispositiu, robar claus privades, accedir a moneders de criptomonedes o moure's lateralment per la xarxa.
- **Ús de videotrucades com a camuflatge**: els ciberdelinqüents fan servir el trànsit de videoconferència per amagar comunicacions de comandament i control.

4. BONES PRÀCTIQUES

COM POTS REDUIR EL RISC?

- Desconfia d'ofertes generoses o propostes d'inversió inesperades.
- Verifica la identitat dels contactes nous, especialment si arriben a través de Telegram, LinkedIn o altres plataformes socials.
- Fes servir canals corporatius verificats per a les comunicacions sensibles.
- Recorda que un compte legítim pot estar compromès.
- Confirma la identitat del remitent a través de canals alternatius abans d'obrir fitxers o enllaços.
- Mai executis scripts o ordres no verificats.

5. *GHOSTCALL* VS. TRUCADA FANTASMA

GhostCall → **Campanya de ciberestafa avançada** atribuïda al grup APT **BlueNoroff** que fa servir **falses reunions de Zoom** o **Microsoft Teams** per infectar equips.

***Vector d'atac**: enllaços maliciosos en invitacions falses a Zoom/Teams.*

- **Enginyeria social**: invitacions falses a videotrucades.
- **Objectiu: comprometre macOS**, robar credencials o actius digitals.
- **Atac dirigit**, sofisticat i amb motivació econòmica.

Trucades fantasma → Les trucades fantasma són un fenomen **molt més ampli i genèric**, relacionat amb **telefonia VoIP** i sistemes SIP. No són una campanya APT concreta.

***Vector d'atac:** trucades SIP automàtiques sense interlocutor.*

- **Sona el telèfon però no contesta ningú.**
- **Escanejos automàtics** de ports SIP, bots o configuracions errònies.
- S'utilitzen com a **reconeixement previ** abans d'atacs VoIP, no impliquen infecció d'equips.
- Afecten qualsevol sistema VoIP, no videoconferències com Zoom o Teams.

El fenomen conegut com a **trucades fantasma** són intents de contacte que no porten a una conversa real, són una nova tàctica emprada pels ciberdelinqüents per dur a terme atacs més sofisticats.

TRUCADA FANTASMA

**No conversa real*

=

INTENTS DE CONTACTE

→

ATACS MÉS SOFISTICATS

Darrere d'aquestes trucades **hi ha robots o sistemes automàtics de marcatge massiu emprats per empreses de telemàrqueting i centres d'atenció telefònica**.

Objectiu

Confirmar que el número està actiu i que existeix un usuari disposat a respondre.

Registrar aquest número com a «vàlid» per a futures campanyes, tant comercials com de telemàrqueting.

Agendar el número per a posteriors intents de venda o contacte.

Respondre o tornar la trucada a un número desconegut = **línia activa i susceptible de rebre noves trucades**.

6. PER QUÈ ES FAN I QUÈ IMPLIQUEN?

Aquestes trucades poden ser només una molèstia, però també indiquen que el **teu número**:

- **Ha sigut inclòs en llistes de *spam*.**
- **Està sent provat per bots per a futures campanyes.**
- **Està rebent trànsit automatitzat que podria augmentar amb el temps.**

En alguns casos, especialment amb VoIP, poden indicar vulnerabilitats de seguretat en la configuració del sistema.

7. RECOMANACIONS

MESURES PER A MÒBILS

Com pots evitar caure en trucades fantasma.

- **Activa el filtre de trucades *spam*** del sistema.
- **Bloqueja els números que es repeteixin**, malgrat que canviïn freqüentment.
- **Evita tornar la trucada** a números desconeguts que pengin a l'instant.
- **Usa una app d'identificació de trucades** (Truecaller, Hiya, etc.) per detectar trucades robotitzades.
- **Activa l'opció «Silenciar trucades desconegudes»** si no esperes trucades noves.

La **MILLOR DEFENSA ÉS LA PREVENCIÓ**, i tant Android com iOS ofereixen eines per filtrar i bloquejar trucades no desitjades.

Android

- **Filtre de trucades**: detecta trucades sospitoses i bloqueja automàticament futurs intents.
- **Identificador de trucada i *spam***: permet visualitzar informació addicional abans de respondre.
- **Silenciament de números desconeguts**: configura el dispositiu perquè només sonin trucades de contactes apuntats a l'agenda.

iOS

- **Filtre de trucades**: analitza la procedència i mostra alertes de possibles riscos.
- **Bloqueig i silenciament**: permet bloquejar fàcilment números no desitjats i silenciar trucades de desconeguts.

RECORDA

Respondre només les trucades de contactes coneguts.

Activar filtres i bloquejadors de trucades en el dispositiu.

Desconfiar de trucades o missatges que generin sensació d'urgència o provinguin de números desconeguts.

Fer servir canals alternatius com el **correu electrònic** o **missatgeria instantània per a contactes importants**.

No tornis la trucada a números que no tinguis registrats a l'agenda.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.