Aicila - Verificar updates de Windows - Microsoft

Autor:
Data de publicació: 01-11-2025

Com distingir si un update de Windows es autèntic..
Hay constancia de algun malware q se haya instalado imitando un update de windows?
Sí: existe malware diseñado exactamente para imitar una actualización de Windows y engañar al usuario para que la descarregui o l'executi. Aquest tipus d'atac és molt comú perquè juga amb la por legítima a no tenir el sistema actualitzat. A continuació tens què cal saber, com identificar-ho i què fer si sospites que t'ha passat

Hay constancia de algun malware q se haya instalado imitando un update de windows?

Sí: existe malware diseñado exactamente para imitar una actualización de Windows y engañar al usuario para que la descarregui o l'executi. Aquest tipus d'atac és molt comú perquè juga amb la por legítima a no tenir el sistema actualitzat. A continuació tens què cal saber, com identificar-ho i què fer si sospites que t'ha passat.

Principals variants i tàctiques (resum)

Missatges o finestres que imiten l'aspecte d'una actualització de Windows però apareixen dins del navegador o com a pop?ups.

Paquets maliciosos que es presenten com a instal·lador d'actualització i que instal·len ransomware, roba de credencials (stealers) o altres backdoors.

Famílies conegudes relacionades amb aquest vector: malware tipus "FakeUpdate" (campanyes que distribueixen ransomware o stealers), troians com RedLine (robadors de credencials) i ransomware que es fa passar per update (per exemple variants informades com "Big Head" o campanyes de "Cyborg").

L'atac pot utilitzar una pàgina web maliciosa, un enllaç de phishing o una extensió del navegador per mostrar la falsa actualització.

Senyals que l'"update" era fals

L’avís va aparèixer dins del navegador (una pestanya o un pop?up), no com a notificació del sistema o des de Configuració > Windows Update.

T’hi demanen que descarreguis un .exe, .msi o .zip des d’una pàgina que no sigui microsoft.com..

Ortografia pobre, logos pixelats, URLs estranyes o botons que redirigeixen a llocs externs.

T’exigeixen permisos elevats immediats (UAC) des d’un fitxer descarregat.

Després de la “instal·lació” el PC va quedar lent, van aparèixer noves icones/serveis desconeguts, xifratge de fitxers o peticions de rescat.

Eines de seguretat donen alertes o es desactiven.

Com comprovar-ho ara mateix (pasos ràpids)

Desconnecta del network (Wi?Fi off / cable fora).

No introdueixis cap dada ni autoritzis res més des d’aquest equip.

Obre Configuració > Actualització i seguretat > Windows Update i comprova l’historial d’actualitzacions.

Revisa Descàrregues i Documents recents i elimina qualsevol instal·lador sospitós.

Escaneja completament amb l’antivirus del sistema i, si pots, amb una segona eina antimalware reconeguda (Malwarebytes, ESET Online Scanner, etc.).

Revisa tasques programades, programes instal·lats i extensions del navegador per detectar elements nous o desconeguts.

Si tens sospites fortes, arrenca en Safe Mode o des d’un medi extern per fer analítica més profunda.

Accions immediates si detectes signes d’infecció

Desconnecta completament l’equip d’internet.

Des de un dispositiu segur, canvia contrasenyes crítiques (bancs, correu, autenticadors) i revisa l’activitat bancària.

Contacta amb el teu banc i informa de la possible exposició; demana bloqueig o vigilància de la compte.

Guarda proves (captures, noms d’arxius, hores) per si cal denunciar.

Si hi ha xifratge o petició de rescat, no paguis sense assessorar?te: consulta amb un professional en seguretat.

Considera restaurar a un punt anterior si és segur o, millor, fer còpia de seguretat de fitxers importants i reinstal·lar Windows des d’un mitjà oficial si no aconsegueixes netejar la infecció.

Prevenció per evitar-ho en el futur

Les actualitzacions només per Windows Update o descàrrega des de microsoft.com..

No descarreguis ni executis .exe/.msi des de pop?ups o webs no oficials.

Mantén navegador i extensions mínims i vigilats; bloqueja pop?ups.

Activa l’UAC i mantén antivirus actualitzat.

Usa autenticació multifactor a banca i correu.

Ten backups externs i comprova que funcionin.

Si vols, t’ajudo ara mateix a:

fer una llista de comprovacions prioritàries pas a pas per executar en el teu equip; o

redactar el missatge clar i tècnic per enviar al servei d'atenció del teu banc (amb indicació d'arxius sospitosos i hores). Quin prefereixes?

Això q dius per evitar els updates seria molt maco QUE SIGUI INICIATIVA DE L'USUARI INICIAR UN UPDATE PERÒ EN REALITAT NO ÉS AIXÍ moltes vegades em trobo la mà quina REINICIADA amb un update instal·lat

Visualitza el meu pensament

Perquè passin les actualitzacions només quan tu vulguis
És frustrant trobar-te l'ordinador reiniciat de forma inesperada. Windows intenta mantenir-se segur instal·lant i reiniciant, però hi ha diverses opcions perquè siguis tu qui control·li quan es baixen i s'instal·len les actualitzacions. A continuació tens mesures pràctiques i segures, ordenades de menys a més intrusives.

Mesures ràpides (fàcils i recomanades)

Posar en pausa actualitzacions

Obre Configuració > Actualització i seguretat > Windows Update > Posar en pausa.

Pots pausar temporalment fins a 7–35 dies segons la versió.

Configurar hores actives

Configuració > Actualització i seguretat > Windows Update > Canviar hores actives.

Windows evitarà reiniciar dins de l’interval que indiquis.

Opció de reinici manual

Si hi ha una actualització pendent, a Windows Update has de veure “Programar el reinici” o “Reiniciar ara / Programar reinici”. Programa-ho quan et vagi bé.

Fer la connexió de xarxa mesurada

Configuració > Xarxa i Internet > Propietats de la connexió > Marcar com a connexió mesurada.

Això evita descàrregues automàtiques d’actualitzacions grans en connexions Wi?Fi.

Controls des d’«Opcions avançades» (més precisos)

Rebre actualitzacions opcionals manualment

Configuració > Windows Update > Opcions avançades > Mostrar actualitzacions opcionals.

Així decideixes si instal·les paquets no crucials.

Deferir actualitzacions de característiques (si està disponible)

A “Opcions avançades” pots retardar les actualitzacions de funcionalitat uns mesos (només en algunes edicions).

Activar avisos i no automàtics

Assegura’t que t’arriben notificacions perquè sàpigues quan hi ha actualitzacions disponibles i hagis de triar instal·lar-les.

Canvis més ferms (Windows Pro / Enterprise — gpedit)
Si tens Windows Pro o superior, tens més control amb l’Editor de polítiques de grup local:

Obre gpedit.msc ? Computer Configuration ? Administrative Templates ? Windows Components ? Windows Update ? Configure Automatic Updates.

Activa la política i tria l’opció 2 – Notificar per descàrrega i notificar per instal·lació. Així serà sempre l’usuari qui iniciï la descàrrega i la instal·lació.

Configura també No auto-restart with logged on users for scheduled automatic updates installations perquè no es faci reinici automàtic mentre hi hagi usuaris connectats.

Opció per a Windows Home (registri — fer còpia abans)
Si tens Windows Home i vols un control similar, es pot canviar el registre (cal fer-ho amb cura i fer còpia de seguretat abans):

Ruta: HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftWindowsWindowsUpdateAU

Valors clau que s’utilitzen habitualment:

NoAutoUpdate = 1 (desactiva actualitzacions automàtiques)

AUOptions = 2 (notificar per descàrrega i instal·lació)

No facis canvis al registre si no et sents còmode; millor demanar ajuda o fer-ho amb instruccions pas a pas.

Altres consideracions i bones pràctiques

Còpies de seguretat: Abans d’aplicar grans actualitzacions (features), fes una còpia de seguretat dels fitxers importants.

Punts de restauració: Crear un punt de restauració abans d'una instal·lació important t'ajuda a revertir canvis si cal.

Evita desactivar completament Windows Update: pot deixar el sistema vulnerable. Les solucions recomanades són pausar i programar, no desactivar permanentment.

Control de reinicis: quan hi hagi actualitzacions pendents, utilitza "Programar reinici" i tria una hora que no interferesqui amb el teu treball.

Mantén antivirus i navegadors actualitzats per evitar que falses finestres d'actualització t'enganyin.

Si vols, et preparo:

els passos exactes per aplicar la política gpedit (amb captures) si tens Windows Pro; o

un petit script o llista d'instruccions pas a pas perquè facis els canvis al registre (si tens Windows Home).