MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Attento a quel Software

I rischi legati all'utilizzo di applicazioni e programmi non autorizzati

Sommario

Cosa troverai in questa brochure

Introduzione

Al giorno d'oggi, grazie alla diffusione di **store online** che offrono un'ampia gamma di **servizi accessibili con pochi clic**, **scaricare** e **utilizzare software** e **applicazioni** sui propri dispositivi è diventato semplice e immediato. Infatti, è possibile scaricare un'ampia varietà di software e applicazioni, da quelle più comuni per la messagistica e social media, fino a quelle dedicate alla gestione della salute, dell'home banking oppure applicativi utili per gestire attività lavorative (es. word, excel, etc.).

La **facilità** di **accesso** a tali applicazioni, sebbene abbia portato numerosi benefici, come la possibilità di effettuare operazioni in modo rapido, comodo e da qualsiasi luogo, di contro ha introdotto **nuove vulnerabilità** e **rischi** per la **sicurezza informatica** (es. download di **malware**). L'uso di **software** e/o **applicazioni** da **fonti non autorizzate** o da siti che offrono versioni gratuite di programmi a pagamento potrebbe rappresentare un **rischio per la sicurezza del tuo dispositivo e per i dati personali ivi contenuti**.

Tipologie di Malware

Il **Malware** è un **software malevolo**, progettato per **rubare dati** e **spiare** le **tue attività,** che può assumere diverse forme, fra le quali, a titolo esemplificativo e non esaustivo:

Spyware: malware creato per raccogliere dati e monitorare le tue attività (es. ricerche, registrazioni audio/video) sui dispositivi, senza consenso.

Trojan: malware che si finge software legittimo, ma nasconde funzioni dannose che aprono una porta nel sistema, dando ai criminali accesso e controllo sui dispositivi.

Ransomware: malware che cifra i dati presenti sul dispositivo avanzando richieste di riscatto per ripristinare l'accesso ai contenuti.

Numerosità di visite su siti pirata

386 Mln

Accessi giornalieri a **siti pirata** dove scaricare software e/o applicazioni (a livello mondiale nel 2023).

141 Mld

Accessi annuali a **siti pirata** dove scaricare software e/o applicazioni (a livello mondiale nel 2023).

Fonte: TorrentFreak Report 2023

Quali sono i rischi?

Rischi

01 Frodi Finanziarie

L'uso di **software** o **applicazioni non ufficiali** può esporti ad **esfiltrazioni** di **dati sensibili**, come credenziali di accesso, numeri di carte e informazioni bancarie. Una volta sottratti, questi dati possono essere utilizzati dai criminali informatici per compiere ulteriori attività fraudolente, tra le quali, le **transazioni finanziarie non autorizzate**, con potenziali gravi conseguenze economiche per la vittima.

02 Violazione Privacy

Programmi scaricati da siti non ufficiali potrebbero esporti a **rischi informatici non** immediatamente **percepibili**, come nel caso di infezioni da malware di tipo **spyware, trojan**, etc. Tali programmi potrebbero avere le medesime funzionalità di quelli originali, ma, se modificati ad arte dai criminali informatici, possono essere utilizzati per sottrarre dati sensibili o monitorare in modo illecito le attività svolte sul tuo dispositivo.

03 Indisponibilità informazioni

L'utilizzo di software ed applicazioni illecite può esporti a gravi rischi di **indisponibilità** delle **informazioni**, dovuti all'azione di specifici **Ransomware**. Il Ransomware è infatti una tipologia di software malevolo progettato per esfiltrare i dati dal tuo dispositivo rendendoli di fatto inaccessibili e causando gravi ripercussioni sulla sicurezza delle informazioni.

Contromisure

Assicurati di utilizzare solo software e applicazioni **scaricati da store ufficiali o dai siti web dei produttori**, per garantire la sicurezza dei tuoi dispositivi

Controlla i **permessi** richiesti per accedere a dati o funzionalità: se l'applicazione impone l'**accesso** a **dati non necessari** per il funzionamento (es. foto, posizione, etc.) potresti essere incorso in software malevolo

Programma **backup regolari** e **automatizzati** per garantire la disponibilità continua di dati e informazioni: in questo modo potrai contare su **copie aggiornate e protette**, pronte all'uso anche in caso di attacchi informatici

03

Come difendersi?

Rispetto dei limiti di licenza

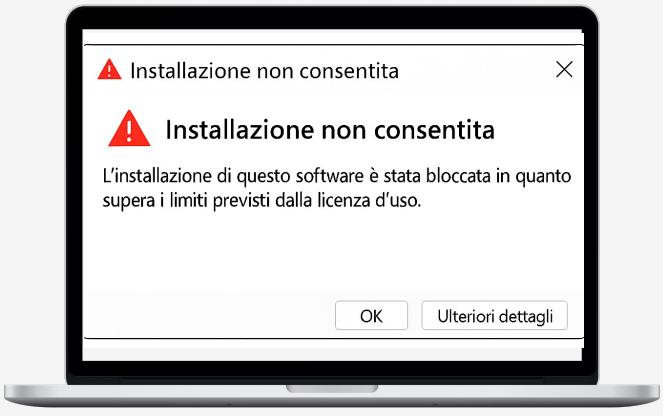
Per non incorrere in **violazioni** del **copyright** e conseguenti **sanzioni amministrative** e **penali**, è fondamentale scaricare e **utilizzare software** e **applicazioni** nel pieno rispetto delle **condizioni** stabilite nella **licenza d'uso.** Un **utilizzo conforme** di tali applicativi, infatti, non si limita ad individuare i soli canali ufficiali dove poter scaricare gli stessi, ma include anche il **rispetto delle restrizioni** sul **numero di dispositivi**, le **finalità di utilizzo**, etc.

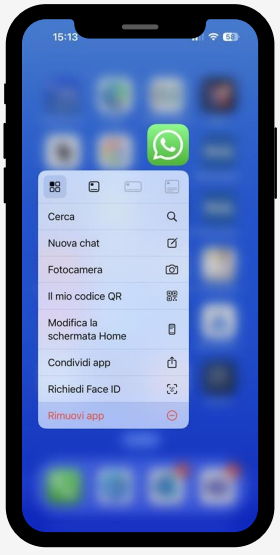
Rimozione di software e programmi

Se ti accorgi di essere incorso in **software** e/o **applicazioni malevole** perché, ad esempio, scaricate da fonti poco affidabili, **rimuovi** immediatamente il **programma** o **l'applicazione** che ritieni **sospetta** dal tuo dispositivo. Successivamente all'eliminazione, **monitora** il **comportamento** del tuo **dispositivo e resetta** tutte le **password** di accesso ad altri servizi. In caso di **anomalie**, **segnalale** prontamente al **reparto IT** del tuo contesto organizzativo di riferimento.

Verifica dei download consentiti

Nel **contesto lavorativo**, prima di **scaricare software** e/o **applicazioni** sui dispositivi che ti sono stati forniti, verifica che gli stessi siano **autorizzati** da **politiche interne**. Il loro download, benché effettuato su store ufficiali, potrebbe **compromettere la sicurezza delle informazioni** della tua organizzazione, esponendo i sistemi a **vulnerabilità** non previste e mettendo seriamente a rischio l'intera infrastruttura di sicurezza informatica.





Security Trend

MalTube: la campagna che ha sfruttato YouTube per veicolare contenuti infetti

Tra l'estate e l'autunno del 2024, è stata diffusa una campagna malevola soprannominata "**MalTube**", che **sfruttava YouTube** per **veicolare contenuti infetti**.

Nello specifico, alcuni criminali informatici hanno diffuso dei **video** su **YouTube** che illustravano alcune **modalità** per **scaricare** dei **software gratuitamente**. In realtà, chi guardava questi video era indotto a **cliccare** su un **link** presente nella descrizione, che rimandava a **siti esterni** creati ad hoc dai truffatori per **distribuire file infetti**.

Il **software** scaricato si presentava come un uno strumento **legittimo**, ma **in realtà** conteneva **malware nascosti**. Una volta avviato, il programma **infettava** il **computer** della vittima, spesso stabilendo un meccanismo di persistenza che gli permetteva di rimanere attivo senza essere rilevato, anche dopo riavvii del sistema.

Questo caso evidenzia l'importanza di **utilizzare solo software/applicazioni scaricate da fonti ufficiali:** affidarsi a canali non autorizzati, nella speranza di risparmiare o ottenere funzionalità aggiuntive, apre spesso la porta a infezioni silenziose, furti di dati sensibili e compromissioni dei sistemi.

novembre 2024

Stop alle app modificate: utenti esclusi da Spotify

Per anni molti utenti hanno usato versioni illegali di app di streaming musicale per **accedere gratuitamente ai servizi premium**.

Tuttavia, lo scorso anno, **Spotify**, colosso svedese dello streaming musicale, ha intrapreso un'azione decisa contro l'uso di **versioni modificate e non autorizzate** della sua applicazione.

Gli utenti che utilizzavano queste versioni per accedere gratuitamente alle funzionalità premium hanno improvvisamente riscontrato **l'impossibilità di utilizzare il servizio**.

Le playlist apparivano vuote e l'accesso alla musica era bloccato. L'azione di Spotify ha mirato a **rafforzare la sicurezza della piattaforma** e a garantire che solo gli utenti autorizzati potessero accedere alle funzionalità esclusive. L'uso di applicazioni modificate non solo **vìola i termini di servizio**, ma espone anche gli utenti a **rischi significativi**, come il **furto di dati personali e finanziari**.

Questo caso evidenzia l'importanza di utilizzare solo **software o applicazioni** nel **rispetto dei limiti di licenza** e delle **condizioni legali** di **utilizzo**: in questo modo si evitano sanzioni amministrative e/o penali derivanti dalla violazione del copyright.

novembre 2024

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.