

Pirateria audiovisiva, a rischio la sicurezza informatica: malware colpisce un milione di dispositivi



Il malware diffuso dai siti di streaming pirata

Negli ultimi anni, i siti e le app di **streaming pirata** sono diventati per le organizzazioni criminali una delle principali fonti di profitto, ricavato dall'intrattenimento illecito di milioni di utenti in tutto il mondo. Tuttavia, dietro l'apparente gratuità di questi servizi si nasconde un rischio sempre più preoccupante per la sicurezza informatica del singolo utente. Un recente rapporto pubblicato da Microsoft Threat Intelligence ha rivelato una **massiccia campagna malware avviata attraverso siti di streaming illegali**, che ha coinvolto un milione di dispositivi in tutto il mondo.

Secondo il Report, l'attacco è stato reso possibile grazie all'uso di **iframe malvertising redirector URLs**, un sistema che genera entrate pubblicitarie reindirizzando gli utenti attraverso una serie di pagine per poi portarli su siti di truffe o di distribuzione malware. Stando a quanto riportato da *torrentfreak.com*, questo processo poteva coinvolgere fino a cinque livelli di reindirizzamento prima che il malware venisse scaricato.

La prima fase dell'attacco si basava su file malevoli ospitati su piattaforme legittime come **GitHub, Discord e Dropbox**. Questi file agivano da "*dropper*", ovvero software progettati per scaricare ulteriori componenti dannosi da altre fonti, permettendo agli hacker di compromettere ulteriormente i dispositivi infetti.

Un attacco a più fasi. Obiettivo finale: rubare dati sensibili e prendere il controllo del dispositivo

L'operazione malevola si sviluppava in più fasi:

1. **Prima fase** – Il malware iniziale veniva scaricato da repository online e installato sul dispositivo della vittima.
2. **Seconda fase** – Il software malevolo raccoglieva informazioni sul sistema, come specifiche hardware e software, che venivano poi inviate a un server remoto.
3. **Terza fase** – In base ai dati raccolti, venivano scaricati ed eseguiti ulteriori script e programmi per garantire persistenza, evasione delle difese del sistema e comunicazione con il server di comando e controllo (C2).
4. **Quarta fase** – I criminali informatici utilizzavano strumenti avanzati per monitorare l'attività

dell'utente, iniettare codice malevolo nei processi attivi, sottrarre dati sensibili e acquisire il controllo remoto del dispositivo.

Furto di informazioni e danni potenziali per conti bancari e identità digitale

Il fine ultimo della campagna malware era il **furto di informazioni sensibili**, tra cui credenziali di accesso, **dati bancari** e altri dettagli personali sempre sfruttabili da un punto di visto economico, tra cui certamente la nostra identità digitale. Tra i software utilizzati per l'attacco spiccavano **Lumma Stealer** e **Doenerium**, noti per prendere di mira videogiocatori e utenti che scaricano mod non ufficiali.

Inoltre, i cybercriminali hanno utilizzato **Living-Off-The-Land Binaries and Scripts (LOLBAS)**, ovvero strumenti di sistema legittimi come PowerShell.exe, MSBuild.exe e RegAsm.exe, per mascherare le proprie attività e sfuggire alle difese antivirus.

Per evitare di compromettere la sicurezza informatica, evitare lo streaming illegale

L'utilizzo di siti di streaming pirata espone gli utenti a numerosi pericoli, tra cui **malware, truffe informatiche e violazioni della privacy**. Per ridurre il rischio di infezione, Microsoft consiglia di adottare le seguenti misure di sicurezza:

- **Evitare i siti di streaming illegali:** sebbene possa sembrare un consiglio ovvio, è la soluzione più efficace per evitare di cadere vittima di attacchi informatici.

- **Utilizzare software di sicurezza affidabili:** antivirus aggiornati, firewall e strumenti di protezione avanzata possono rilevare e bloccare minacce prima che possano causare danni.
- **Abilitare la protezione di rete e il Tamper Protection:** queste impostazioni di sicurezza avanzate impediscono modifiche non autorizzate al sistema operativo e bloccano il traffico sospetto.
- **Evitare il salvataggio delle credenziali nei browser:** l'uso di un gestore di password crittografato è preferibile rispetto al salvataggio di dati di accesso in chiaro.
- **Mantenere il sistema e i software sempre aggiornati:** le patch di sicurezza rilasciate dai produttori di software correggono vulnerabilità sfruttabili dai cybercriminali.
- **Utilizzare un Ad Blocker avanzato:** ridurre l'esposizione agli annunci malevoli può diminuire il rischio di reindirizzamenti verso siti infetti.
- **Navigare in ambienti isolati:** se si desidera esplorare siti web potenzialmente rischiosi, utilizzare macchine virtuali o sistemi operativi dedicati per evitare che un'infezione comprometta il computer principale.

La pirateria è un reato: non danneggia solo l'industria audiovisiva e delle dirette live di eventi sportivi, ma colpisce anche i singoli utenti

Lo streaming illegale di contenuti protetti da copyright non è solo una questione legale, perché va a danneggiare gli investimenti del settore, i ricavi dell'industria e mette a rischio centinaia di migliaia di posti di lavoro, ma rappresenta anche un grave pericolo per la sicurezza

informatica degli utenti.

Come ha suggerito più volte **Federico Bagnoli Rossi**, Presidente della FAPAV – Federazione per la Tutela delle Industrie dei Contenuti Audiovisivi e Multimediali: *“Per contribuire ad affrontare questo problema, è necessario cambiare anche l’atteggiamento dei consumatori, a partire dai rischi di sicurezza informatica e di violazione della privacy, spesso ignorati o sottovalutati, nonché sui danni economici causati dalla fruizione illegale. Anche per questo è sempre più importante realizzare campagne di comunicazione e di educazione rivolte al grande pubblico per incentivare la scelta di offerte legali disponibili sul mercato e con l’obiettivo di diffondere una cultura della legalità, imparando a riconoscere nella creatività e nella Proprietà Intellettuale un valore per tutti”*.

La campagna malware in questione evidenzia come i siti pirata possano diventare vettori di attacchi sofisticati, mettendo a rischio milioni di dispositivi in tutto il mondo e creando danni irreparabili agli stessi proprietari (una volta che i nostri dati sensibili sono stati sottratti e i nostri conti bancari violati non si torna indietro).

Adottare un comportamento responsabile online, utilizzare fonti legittime per la fruizione dei contenuti audiovisivi digitali (dalla tv ai film, fino alle partite di calcio e altri eventi sportivi o spettacoli live) e implementare adeguate misure di sicurezza sono passi fondamentali per proteggersi dalle minacce informatiche sempre più diffuse. Il prezzo della “gratuità” dei contenuti pirata può essere molto più alto di quanto si immagini.

Leggi le altre notizie sull’home page di Key4biz

<https://www.key4biz.it/pirateria-audiovisiva-a-rischio-la-sicurezza-informatica-malware-colpisce-un-milione-di-dispositivi/524190/>