

Zoom: il punto della situazione sulla sicurezza

Apr 16, 2020 Marco Schiaffino Gestione dati, Hacking, In evidenza, News, Privacy, RSS, Vulnerabilità 0

Tra allarmi, bufale e zoombombing, il software di videoconferenza è al centro delle cronache. E spuntano zero-day in vendita per 500.000 dollari.

È passato da 10 a 200 milioni di utenti in un paio di settimane e i problemi di sicurezza non sono mancati. Capire quale sia l'attuale livello di affidabilità di **Zoom**, però, è difficile anche per gli addetti ai lavori. Proviamo a fare il punto della situazione sulla base di quanto è emerso fino a ora.

Il rispetto della privacy

Gli allarmi per la possibilità che la stessa azienda con sede a San Jose rastrellasse informazioni sensibili attraverso la sua piattaforma, addirittura **usando le trascrizioni delle videoconferenze**, sono circolate per qualche giorno ma si sono dimostrate infondate.

Come abbiamo spiegato in questo articolo, le condizioni di utilizzo di Zoom prevedono esplicitamente che non sia raccolta alcuna informazione dai dati trasmessi e ricevuti nelle conversazioni. Il riferimento a una raccolta di dati a scopo di marketing si riferivano infatti al sito (e ai soliti cookie) e non alla piattaforma.

Qualche polemica è sorta invece riguardo alla possibilità che alcune connessioni passassero per i datacenter situati in Cina. Un fatto che ha sollevato preoccupazioni soprattutto tra

gli utenti che abitano in paesi vicini (Taiwan ha addirittura messo al bando il software) e che temono che i loro dati possano essere intercettati dalle autorità di Pechino.

Dal 18 aprile, l'azienda permetterà ai suoi utenti con licenza a pagamento di impostare il routing dei dati in modo da avere la certezza di evitare "passaggi a rischio" come quelli attraverso i datacenter cinesi.

Zoom, è bene ricordarlo, non utilizza un sistema di crittografia end to end, ma una "semplice" crittografia TLS come quella usata da tutte le connessioni su protocollo HTTPS. La preoccupazione per un'eventuale intercettazione, quindi, non completamente infondata e rende il suo utilizzo sconsigliabile per comunicazioni particolarmente riservate.

Riservatezza e impostazioni

I problemi non sono mancati, invece, nella gestione delle videoconferenze. Soprattutto nelle prime settimane di "boom" nell'utilizzo del software, la sua architettura ha mostrato limiti piuttosto evidenti.

La procedura predefinita per l'avvio di una sessione di Zoom prevedeva infatti la creazione di una URL che consentiva il collegamento a chiunque la conoscesse. Il risultato è stato la

nascita del fenomeno del cosiddetto **zoombombing**, cioè la pratica di fare irruzione in videoconferenze per disturbarle con interventi inappropriati che, nella maggior parte dei casi, hanno avuto carattere goliardico.

A spingere il fenomeno è stato, più che altro, l'utilizzo di Zoom per gestire la didattica a distanza nel periodo di distanziamento sociale. Molti studenti, infatti, hanno pensato di approfittare della situazione per giocare qualche scherzo agli insegnanti, organizzando anche dei veri e propri canali dedicati su Discord per distribuire i collegamenti alle videoconferenze.

Dalle parti di Zoom hanno reagito modificando le impostazioni predefinite, introducendo l'uso di una password come procedura "normale" per la creazione della conferenza e abilitando, allo stesso modo, la funzione della waiting room, che lascia in attesa i partecipanti fino a quando l'host della conferenza non ne approva la partecipazione.

Furto di credenziali

Tra gli allarmi circolati in questi giorni, c'è anche quello che vedrebbe un massiccio attacco hacker che avrebbe portato al furto di **500.000 credenziali di utenti Zoom che sono finite in vendita sul Dark Web**.

Se la notizia è stata confermata da numerose società di sicurezza, le conclusioni tratte da alcuni organi di stampa riguardo una presunta vulnerabilità di Zoom sono invece ben poco fondate.

Secondo gli esperti che hanno individuato i database in questione, infatti, si tratterebbe di username e password ottenuti attraverso tecniche di credential stuffing, cioè attraverso l'uso di combinazioni di username e password che gli utenti hanno utilizzato anche in altri servizi e che erano già in circolazione nei bassifondi di Internet.

Il tema della sicurezza, però, è qualcosa con cui dalle parti di Zoom hanno deciso di prendere sul serio. Per farlo, l'azienda si è rivolta ad **Alex Stamos**, esperto di sicurezza che ha lavorato in passato con **Yahoo!** (in uno dei periodi meno felici dell'azienda statunitense) e con **Facebook**.

Il suo intervento potrà consentire qualche correzione relativa ai rischi dell'uso di link all'interno della chat (abbiamo parlato dei rischi in questo articolo) e a una più complessiva revisione dell'architettura del software che sembra ancora piuttosto debole.

Le falle di sicurezza

Tutto bene quindi? No. Perché qualche vulnerabilità "reale" Zoom ce l'ha. Le uniche di cui si conoscono i dettagli (qui il pirotecnico report che le illustra) riguardano la possibilità di un attacco locale su sistemi macOS.

Il vero allarme, però, è arrivato oggi con la notizia riportata da **Motherboard** riguardante la disponibilità di un

exploit zero-day che sfrutterebbe una vulnerabilità critica del client per Windows. Il bug, di cui non si conoscono i dettagli tecnici, consentirebbe di avviare l'esecuzione di codice in remoto. **Tradotto: permetterebbe di usare Zoom come vettore per un attacco malware.**

Stando a quanto viene riportato nell'articolo, l'exploit sarebbe in vendita al prezzo di **500.000 dollari** su quelli che possiamo considerare "mercati informali" del Dark Web. Una quotazione che non stupisce più di tanto, visto che piattaforme "legali" che si occupano di compravendita di exploit come la famigerata **Zerodium** arrivano a offrire fino a 2,5 milioni di dollari per gli exploit sui sistemi e software più diffusi.

Sempre stando alle fonti contattate da Motherboard, esisterebbe poi un altro exploit, relativo però al client per macOS. Insomma: Alex Stamos e i suoi colleghi si trovano ad affrontare una situazione tutt'altro che facile. Il suggerimento, per il momento, è quello di eseguire regolarmente gli aggiornamenti di Zoom per avere la certezza di utilizzare la versione più sicura del software.

Condividi l'articolo

EDP colpita dal ransomware RagnarLocker. Riscatto da 10 milioni

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/04/16/zoom-il-punto-della-situazione-sulla-sicurezza/?utm_source=rss&utm_medium=rss&utm_campaign=zoom-il-

punto-della-situazione-sulla-sicurezza