Eventi
News
Rassegna Stampa
Comunicati Stampa
Video

Ultime News

Certificati SSL: cosa acquistare e perché farlo

Cognitive Security Operation Center

Convention Var Group: tutto il materiale dell'evento

Eventi in programma

Intelligenza Artificiale: come usarla per far crescere il business con Var Group e IBM

Grave vulnerabilità in Microsoft Office sfruttata dal gruppo Cobalt

NEWS

Una **campagna di malware**, riconducibile al gruppo di cybercriminali Cobalt, sfrutta una storica vulnerabilità di Microsoft Office che permette di **avviare codice malevolo all'apertura di un documento**, senza che sia necessaria alcuna interazione con l'utente.

Si tratta di una vulnerabilità grave - **CVE-2017-11882** - perché può essere sfruttata per assumere il controllo completo su un sistema e riguarda le seguenti versioni:

Micro Office 2007 SP3
Microsoft Office 2010 SP2 (32 bit)
Microsoft Office 2010 SP2 (64 bit)
Microsoft Office 2013 SP1 (32 bit)
Microsoft Office 2013 SP2 (64 bit)
Microsoft Office 2016 (32 bit)
Microsoft Office 2016 (64 bit)

La patch che corregge la vulnerabilità è già stata rilasciata da Microsoft lo scorso 14 novembre ma un numero significativo di utenti ha lasciato i loro sistemi senza patch, rendendoli vulnerabili a tali attacchi.

COME AVVIENE L'ATTACCO

I cybercriminali hanno iniziato a diffondere il malware tramite **email di spam** dopo pochi giorni dalla scoperta della vulnerabilità. Il flusso può essere schematizzato nel seguente modo:

Apertura di email malevola creata ad arte e contenente un **file con estensione RTF**. Una volta aperto, il file contatta il server dove è ospitata la prima parte del payload.

Viene quindi eseguito il download della parte successiva, che provvede a scaricare la DLL corretta per l'architettura di sistema.

COME DIFENDERSI

Una delle strategie possibili per mitigare il rischio di questa singola tipologia di attacco è quello di bloccare l'IP 104.254.99.77.

È in ogni caso raccomandato applicare con urgenza le patch di sicurezza rilasciate di Microsoft per evitare che la stessa vulnerabilità venga sfruttata anche in futuro.