Attenzione alla carta di credito che avete salvata su Chrome: un malware ruba i dati!

https://www.hwupgrade.it/i/n/EmotetMalware_720.jpg,

Scoperto un malware capace di rubare i dati sensibili della carta di credito salvati nella cache del browser Chrome. Ecco come funziona e come difendersi.

di Bruno Mucciarelli pubblicata il **16 Luglio 2022**, alle **16:01** nel canale Web

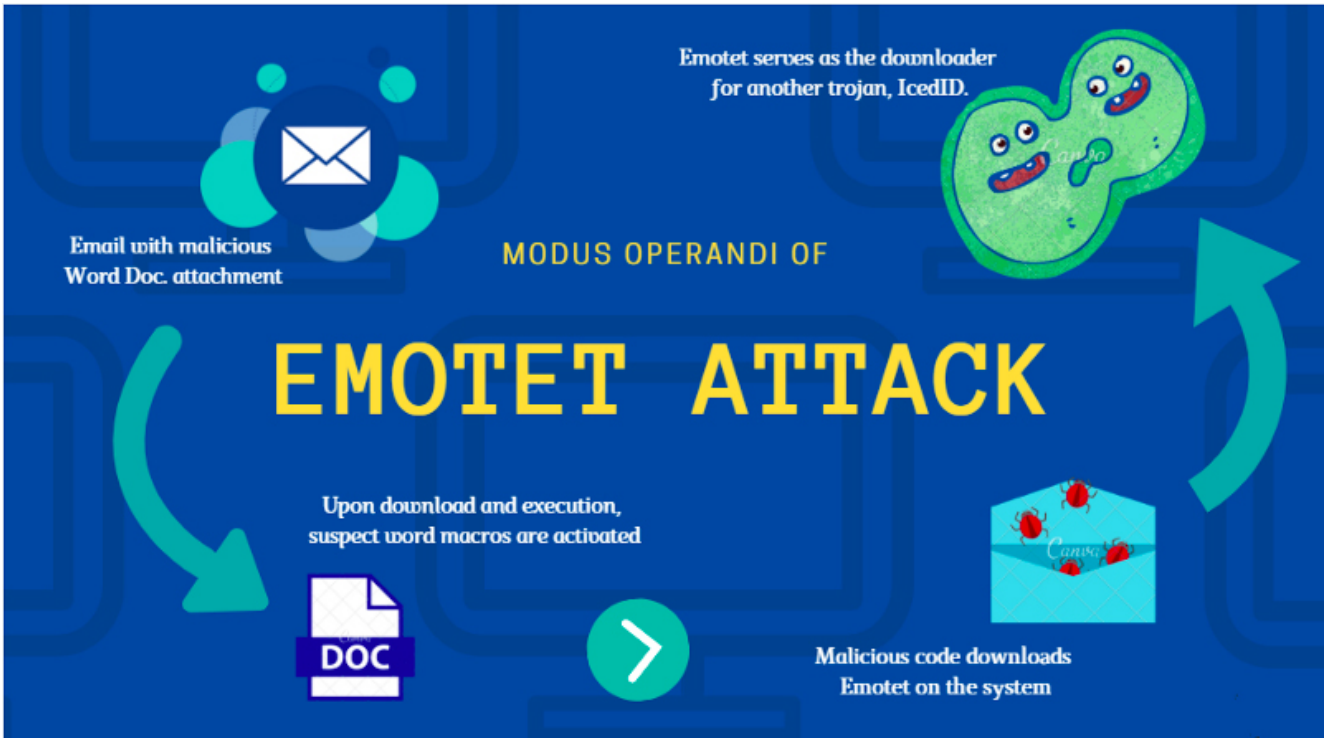
Chrome

Il furto di dati sensibili sul web è una piaga non facile da risolvere e soprattutto molto estesa vista la facilità con cui è possibile realizzarla. Sono oggi sempre di più i malintenzionati che cercano quotidianamente di rubare identità, hackerare email e profili social ma anche e soprattutto **rubare i dati delle carte di credito** per poterle clonare o effettuare acquisti all'insaputa del proprietario.

Proprio in base a questo e ai dati delle carte di credito che usiamo sul web per fare acquisti sui vari negozi online, c'è una pratica molto usata per velocizzare l'operazione che sarebbe meglio evitare d'ora in avanti. Capita sempre più spesso infatti di **salvare i dati della carta di credito nella cache del browser** di Google Chrome. Una pratica comoda che permette agli utenti di trovare subito a portata di mano i dati di pagamento senza dover ogni volta reinserire il numero della carta di credito. Un'operazione sicura almeno fino ad oggi visto che i ricercatori del team **Proofpoint Threat Insights** hanno scoperto un nuovo malware capace di rubare i dati salvati nella memoria cache del browser Chrome.

Chrome: ecco come funziona il malware che ruba i dati

La scoperta è arrivata dai ricercatori del team **Proofpoint Threat Insights** che avevano lanciato l'allarme già alcune settimane fa. In questo caso sembra essere un nuovo modulo di **Emotet**, uno dei malware più diffusi e infestanti degli ultimi anni, pronto a rubare i dati sensibili della carte di credito come numero, intestatario e codice CVV salvati nella cache del browser Google Chrome.



Il suo funzionamento è semplice ma anche efficace per i malviventi. Il malware infatti, dopo aver rubato le informazioni, le invierebbe a server di comando e controllo «C2» diversi rispetto a quelli già utilizzati in genere dallo stesso modulo Emotet per rubare i dati delle carte. Questo renderebbe ancora più difficile risalire ai responsabili del furto informatico.

Una minaccia seria e che per fortuna al momento prenderebbe di mira soltanto i dati memorizzati nella cache del browser di Google Chrome. Il nuovo malware rischia però di portare in futuro conseguenze ben più spiacevoli. Sappiamo infatti che in passato le infezioni causate da **Emotet** possono introdurre nei dispositivi infetti anche nuovi **ransomware**, programmi che rendono inaccessibili alcuni dati o funzionalità del dispositivo. In questo caso i malintenzionati potrebbero poi richiedere il pagamento di un riscatto, quasi sempre in criptovaluta, per restituire o far ritornare funzionante un dispositivo.

Emotet: come difendersi dal malware?

A differenza di altri virus già noti e che dunque i moderni antivirus sono in grado di bloccare, in questo caso il malware è più complesso e dunque può sviare dagli antivirus. In questo caso dunque si deve mettere in atto la necessità di considerare alcune accortezze da poter adottare per evitare il furto dei dati sensibili. In primis è palese che sia **meglio non salvare i dati della carta di credito nella memoria cache del browser**, ma inserirli a mano ogni volta. Non solo perché secondo gli esperti è necessario fare molta attenzione ai link sui quali si clicca perché questi **malware Emotet** si diffondono in genere tramite email, utilizzando link e allegati pericolosi.

Sull'origine di Emotet ci sono pareri contrastanti. L'Intelligence di Australia, Canada, Nuova Zelanda, Regno Unito e Usa lo avevano accostato ad hacker russi che per questo dopo lo scoppio del **conflitto in Ucraina** avrebbero inasprito gli attacchi. La prima volta Emotet è apparso nel 2014 come trojan bancario poi successivamente sono stati aggiunti moduli che gli consentono di rubare i dati sensibili dei poveri malcapitati.

Read More