Varenyky: è arrivato il “trojan a luci rosse”

Ago 09, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, Privacy, RSS 0

Individuato in Francia, il malware controlla la navigazione della vittima e registra un video dallo schermo se visita un sito pornografico. Obiettivo estorsione?

L’inventiva dei cyber-criminali, in alcuni casi, è davvero ammirevole. Pur di spremere qualche euro alle loro vittime sono infatti capaci di inventarsi qualsiasi tipo di truffa e attacco, modificando le loro strategie in base alle esigenze del momento.

Il caso del trojan **Varenyky**, individuato dai ricercatori di **ESET**, è la dimostrazione di questa straordinaria capacità di fiutare un nuovo “affare”, puntando a estorcere denaro agli sventurati che ne finiscono vittima.

Come spiegano i ricercatori in un report pubblicato sul blog della società di sicurezza, Varenyky è comparso in Francia e viene distribuito attraverso una campagna di spam via email che cerca di attirare le potenziali vittime con classiche tecniche di phishing.

Nel dettaglio, il messaggio in francese fa riferimento a una presunta fattura da 491,27 euro ed è scritto con una certa cura.

Il trojan viene installato quando la vittima apre il documento **Word** allegato, che richiede la solita attivazione delle macro mascherata, in questo caso, come un sistema di verifica per superare la protezione del documento e consentirne l'apertura.

Gli autori del malware, inoltre, hanno introdotto un piccolo accorgimento per renderne più difficile l'individuazione da parte dei sistemi di scansione automatica. **Prima di avviare l'installazione, infatti, i comandi macro verificano le impostazioni di Word per controllare che sia impostato per la lingua francese**.

Nel caso in cui la lingua sia un'altra, o sia impostata sulle versioni pensate per altri paesi francofoni come Belgio o Canada, l'esecuzione del codice si blocca.

Un ulteriore controllo, questa volta relativo al layout di tastiera, viene effettuato all’inizio dell’esecuzione del codice del trojan.

La logica è semplice: quando il file finisce su un computer impostato con un’altra lingua (per esempio quelli usati dalle società di sicurezza per analizzare i file intercettati su Internet) il documento appare innocuo.

Le funzionalità di Varenyky comprendono moduli classici, come il furto delle credenziali di accesso ai servizi Internet, ma anche uno strumento piuttosto originale. Il trojan, infatti, esegue un monitoraggio della navigazione su Internet.

Obiettivo: individuare il momento in cui il proprietario del computer si collega a un sito con materiale pornografico.

Quando questo avviene (il malware verifica una serie di parole chiave) Varenyky attiva un sistema di registrazione dello schermo attraverso **FFmpeg**, che lo stesso trojan scarica e avvia. **Il video viene poi inviato al server Command and Control gestito dai pirati informatici**.

L'obiettivo, anche se i ricercatori di ESET usano il condizionale, è probabilmente quello di utilizzare il video per ricattare la vittima, minacciando di rendere pubblico il video nel caso in cui non paghi un riscatto.

Insomma: si tratterebbe di una nuova versione della **truffa a luci rosse**, di cui abbiamo parlato ampiamente in passato e che sembra aver fruttato centinaia di migliaia di dollari ai suoi autori.

Nel caso della truffa a luci rosse, però, il ricatto si basava su un bluff. Con Varenyky le cose vanno decisamente peggio, visto che in questo caso gli estortori avrebbero veramente tra le mani un video compromettente.

Condividi l'articolo

Il 5G è agli esordi ma ci sono già problemi di sicurezza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/09/varenyky-e-arrivato-il-trojan-a-luci-rosse/