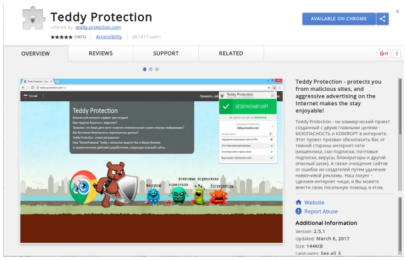

I ricercatori di ESET hanno identificato Stantinko, una backdoor modulare che attraverso un complesso sistema di infezione spinge le vittime (finora oltre 500.000) ad installare due estensioni per il browser, ‘The Safe Surfing’ e ‘Teddy Protection’, entrambe disponibili sul web store di Google Chrome.

Una volta installato, Stantinko è in grado di creare account fake su Facebook che possono mettere “Mi piace” sulle immagini, sulle pagine e addirittura aggiungere amici.

Queste estensioni sembrano a prima vista legittime ma, una volta installate, ricevono una configurazione differente che contiene delle indicazioni per effettuare numerose attività fraudolente, come ricerche anonime su Google per trovare siti sviluppati con Joomla e WordPress ed eseguire attacchi brute force su di essi, generare falsi clic ed inserire annunci pubblicitari non desiderati, ottenendo in questo modo un ritorno economico da tutto il traffico fornito agli inserzionisti.

La capacità di Stantinko di evitare la rilevazione degli antivirus si basa su sofisticate tecniche di offuscamento e sulla possibilità di nascondersi dietro codici che sembrano legittimi; è difficile poi liberarsene perché ogni modulo da cui è composto ha la capacità di reinstallare l’altro nel caso venisse eliminato dal sistema. Per risolvere del tutto il problema, l’utente deve eliminare contemporaneamente entrambi i moduli
.

Per ulteriori informazioni su Stantinko è possibile visitare il blog di ESET Italia a questo link

{jcomments on}

{loadposition user6}