# Spyware su Google Chrome, cosa sono e come si diffondono i captatori informatici

Un report della società di sicurezza informatica **Awake Security** ha scoperto che **Google Chrome** è stato sfruttato per una massiccia operazione di **spyware**. I cybercriminali hanno usato le estensioni di Chrome, il browser di gran lunga più usato al mondo con una quota del mercato globale di circa due terzi (64%), per infettare milioni di computer.

## Come è avvenuto

Tali estensioni, scaricate 32 milioni di volte, sulla carta si presentavano come strumenti gratuiti per normali attività, ad esempio per convertire un file da un formato a un altro. In realtà erano spyware in grado di carpire la cronologia di navigazione in rete e le credenziali per accedere a strumenti aziendali interni.

Come ha riportato la Reuters, Google ha dichiarato di aver eliminato una settantina di queste estensioni dal negozio ufficiale per Chrome il mese scorso, dopo essere stato avvisato dagli esperti di sicurezza.

## Spyware: cosa sono e come si diffondono

Per spyware o captatore informatico si intende un software,

spesso sotto forma di virus trojan, in grado di raccogliere informazioni e dati. A differenza dei virus e dei worm, gli spyware non sono in grado di diffondersi autonomamente, ma richiedono l'intervento dell'utente per essere installati.

Il termine spyware è solitamente usato per definire un'ampia gamma di malware, ossia software maligni, dalle funzioni più diverse, quali, ad esempio, l'invio di pubblicità non richiesta (spam), la modifica della pagina iniziale o della lista dei Preferiti del browser, oppure attività illegali quali la re-direzione su falsi siti di e-commerce (phishing).

Molti programmi offerti "gratuitamente" su Internet celano in realtà un malware: il software è apparentemente gratuito, il prezzo da pagare è un'invasione della privacy dell'utente, quasi sempre inconsapevole. Spesso, la stessa applicazione che promette di liberare dagli spyware è essa stessa uno spyware o ha in realtà installato spyware.

Questi malware, quindi, si celano spesso, all'interno di altri programmi apparentemente innocui e vanno a infettare il device target. Il captatore informatico non viene individuato dai sistemi antivirus dei device ove viene allocato, poiché utilizza delle tecniche di mascheramento in grado di eludere i sistemi di rilevamento.

Talvolta, uno spyware può essere installato su un device di un inconsapevole utente sfruttando le usuali tecniche di ingegneria sociale, che utilizzano metodi di comunicazione e di persuasione allo scopo di ottenere o compromettere informazioni personali, tramite un vero e proprio studio di ogni soggetto da intercettare.

# Come viene inviato

Alcuni spyware vengono eseguiti solo nel momento in cui si utilizza l'applicazione di cui fanno parte e con cui sono stati installati e, dunque, la loro esecuzione cessa nel

momento in cui viene chiuso il detto programma. Molti spyware hanno, invece, un comportamento più invasivo poiché modificano il sistema operativo del computer ospite in modo da essere eseguiti automaticamente ad ogni avvio. In certe circostanze, l'installazione di spyware viene eseguita in maniera ancora più subdola, attraverso pagine Web realizzate appositamente per sfruttare le vulnerabilità dei browser o dei loro plug-in. Si parla, in questo caso, di drive by download (o installazione tramite exploit).

Il captatore viene generalmente inoculato con diverse modalità:

- mediante posta elettronica: il *malware* appare come un allegato apparentemente innocuo di posta elettronica;
- mediante web: il *virus* è trasmesso tramite un download effettuato dall'utente da una pagina web;
- mediante trasferimento fisico tramite CD-ROM o un'unità USB da collegare all'apparecchio da infettare;
- mediante infezione dall'esterno attraverso connessione dal *provider* di telecomunicazioni, falsi *update* o siti civetta, oppure tramite IMSI Catcher, anche portatili, che permettono alle forze dell'ordine di portare attacchi di tipo "*man-in-the-middle*" (MTM). Per ragioni di opportunità riguardo le procedure di attacco "istituzionali", si omettono ulteriori dettagli concernenti le tecniche di inoculazione, il cui stato dell'arte si trova in continua evoluzione per via delle "contromisure" di sovente utilizzate dai *target* per aggirare infezioni.

# Spyware e tecniche di contagio

Una volta inoculato all'interno del sistema, il captatore può svolgere diverse attività e funzioni, tra le quali:

- intercettare chiamate vocali, *chat*, SMS, messaggi istantanei, e-mail;

- catturare immagini dallo schermo del dispositivo;
- acquisire la cronologia telefonica e la lista dei contatti;
- intercettare ciò che viene digitato sulla tastiera del *device*;
- visualizzare la cronologia delle ricerche web e "catturare" le schermate visualizzate sul dispositivo;
- registrare le telefonate effettuate anche mediante applicazioni o programmi (per es. Skype);
- effettuare *download* e *upload* di *file* sul dispositivo stesso;
- realizzare intercettazioni di tipo ambientale con attivazione del microfono;
- mettere in funzione la foto-videocamera di telefoni o computer per vedere i volti delle persone vicine;
- sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati;
- svolgere funzioni di *key logger*;
- entrare nella rete domestica dell'utente, attraverso la password del Wi-Fi, e fare ulteriori intercettazioni.

*Spyware su Google Chrome, cosa sono e come si diffondono i captatori informatici*