# Il trojan Stealth Falcon sfrutta le funzioni di Windows Update

Set 10, 2019 Marco Schiaffino In evidenza, Malware, Minacce, News, RSS 0

---

***La nuova versione del malware utilizza il servizio BITS per comunicare con il server Command and Control aggirando firewall e antivirus.***

È in circolazione da almeno 7 anni, ma non smette di evolversi. Stiamo parlando di **Stealth Falcon**, un trojan comparso nel 2012 che oggi utilizza nuove tecniche di comunicazione in grado di renderne ancora più difficile l'individuazione.

Stealth Falcon è un classico strumento di cyber-spionaggio ed è stato utilizzato in passato per colpire dissidenti politici nell'area mediorientale.

Secondo **Citizen Lab**, che già nel 2016 ha pubblicato un'inchiesta sulla vicenda legata a un attacco che aveva preso di mira il giornalista **Rori Donaghy**, si tratterebbe di uno strumento utilizzato dai servizi segreti degli **Emirati Arabi Uniti**.

Un collegamento confermato anche da un'altra inchiesta, questa volta pubblicata da **Reuters** nel gennaio di quest'anno, che anche se usa un altro nome (**Project Raven**) sembra riferirsi allo stesso gruppo di cyber-spioni, composto da **ex-agenti della NSA** reclutati dal governo degli Emirati Arabi Uniti.

Un background che spiegherebbe il livello di sofisticazione

del malware, che in un report di **ESET** viene definito come un malware che dimostra un "approccio sistematico alla raccolta di dati, la loro esfiltrazione, alla possibilità di aggiungere ulteriori strumenti e aggiornare la sua configurazione".




I comandi a disposizione dei cyber-spioni sono piuttosto elementari. Il vero elemento su cui si concentra l'attenzione dei ricercatori di ESET, però, è la tecnica usata da Stealth Falcon per comunicare con i server Command and Control.

Al posto di usare una "semplice" backdoor, il malware sfrutta infatti il servizio **BITS** (**Background Intelligent Transfer Service**) di Windows. Si tratta di una funzionalità utilizzata principalmente per gli aggiornamenti del sistema operativo e di alcuni software, oltre che dai programmi di messaggistica.

BITS è progettato per ottimizzare il trasferimento dei dati, consentendo di spostare grandi quantità di informazioni senza congestionare la rete. **Le comunicazioni di Stealth Falcon, quindi, hanno una buona probabilità di passare inosservate, anche quando il trojan trasmette al server C&C grandi quantità di dati**.

Non solo: considerando la funzione “normale” di BITS, le comunicazioni di questo servizio sono di solito autorizzate automaticamente dal firewall. Il trasferimento, inoltre, viene ripreso automaticamente anche in caso di blocco temporaneo della rete, riavvio della macchina o disconnessione dell’utente.

**Insomma: si tratta in buona sostanza di un canale preferenziale con caratteristiche perfette per garantire l’efficacia delle comunicazioni verso il server controllato dai pirati informatici**.

Oltre all’utilizzo di BITS, Stealth Falcon si distingue anche per un’altra particolarità. Prima dell’avvio del payload principale, infatti, il malware importa una gran quantità di dati dal sistema infetto, che poi non utilizza.

Secondo i ricercatori di ESET potrebbe rappresentare una tecnica di evasione, che punta a “confondere” eventuali sistemi antivirus.

Condividi l’articolo

---

Toyota vittima di una truffa via email. Rubati 37 milioni di dollari

---

## Articoli correlati

## Altro in questa categoria

---

https://www.securityinfo.it/2019/09/10/il-trojan-stealth-falcon-sfrutta-le-funzioni-di-windows-update/