Attacchi a 360 gradi con il rootkit Scranos

Apr 17, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS, Trojan 0

Il malware è in grado di caricare payload in memoria e cancellarli per evitarne il rilevamento. Obiettivo: incassare denaro in qualsiasi modo possibile.

Ha colpito prima in Cina, ma adesso si sta diffondendo in tutto il mondo attraverso una campagna di attacchi che, secondo i ricercatori di **Bitdefender**, rischia di allargarsi a macchia d'olio. **Scranos**, d'altra parte, ha tutte le caratteristiche per avere un certo successo nel settore.

Si tratta di un **rootkit** che utilizza per l'installazione un certificato digitale valido, probabilmente rubato, e che integra una serie di funzionalità in continua evoluzione. Gli stessi ricercatori lo definiscono un "work in progress", che sembra evolversi mano a mano che i suoi autori aggiungono nuovi moduli e payload.

Come spiegano dalle parti di Bitdefender in un report pubblicato dalla società di sicurezza, Scranos ha caratteristiche uniche. Si tratta infatti di un rootkit multi-piattaforma che i pirati informatici diffondono inserendone il codice all'interno di software legittimi (come i reader per e-book) o nei classici crack per videogiochi o software.

Una tecnica piuttosto efficace, visto che i cyber-criminali non devono nemmeno preoccuparsi di utilizzare exploit o vulnerabilità per installare il malware, ma possono "introdurlo" in un processo di installazione avviato direttamente dall'utente.

L'uso del certificato digitale registrato a nome di **Yun Yu Health Management Consulting**, una società con sede a Shangai, gli permette di aggirare i controlli e mantenere un basso profilo.

Nel dettaglio, l'attacco sfrutta un processo distinto in varie fasi, che i ricercatori di Bitdefender hanno analizzato e descritto nel dettaglio.

Il primo componente installato è il dropper, che si preoccupa per prima cosa di rubare alcune informazioni come cookie, credenziali di login e pagamento attraverso delle DLL specializzate che prendono di mira in particolare **Facebook**, **Amazon** e **Airbnb**.

Lo stesso dropper si occupa poi di installare il rootkit sul sistema, che viene avviato a ogni accensione del dispositivo grazie a una modifica del registro.

A questo punto Scranos utilizza il collegamento con il server Command & Control per scaricare e avviare differenti payload, che il rootkit può gestire sotto ogni aspetto. In particolare Scranos adotta una tecnica piuttosto raffinata per far passare inosservata l'attività dei vari moduli che carica, iniettandoli all'interno del processo **svchost.exe**.

I payload individuati dai ricercatori sono estremamente variegati e comprendono la possibilità di promuovere canali **YouTube** attraverso Chrome, rubare le credenziali del servizio di gaming **Steam**, utilizzare l'account di **Facebook** per inviare spam e collegamenti ad app mobile infette, sottrarre i dati riguardanti la cronologia di navigazione su Internet.

Scranos, poi, dedica una particolare attenzione a **Chrome**, installando una serie di estensioni che hanno l’obiettivo di modificare il motore di ricerca predefinito e attirare la vittima su siti pericolosi, presumibilmente controllati dagli stessi pirati informatici o da loro affiliati.

Insomma: per gli autori di Scranos, le vittime sono come il maiale: non si butta via niente. Considerato l’impianto di base del rootkit, però, è probabile che in un prossimo futuro potremo vedere ulteriori evoluzioni.

Please follow and like us:

Falla negli smartwatch TicTocTrack e i pirati possono tracciare i bambini

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/17/attacchi-a-360-gradi-con-il-rootkit-scranos/