

# ServHelper raddoppia: oltre alla backdoor installa un miner

Lug 13, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

---

*La nuova versione del trojan integra un generatore di cripto-valuta che viene installato sul sistema infetto in un ambiente virtuale.*

Perché limitarsi a rubare informazioni quando, nel frattempo, si può anche raggranellare qualche dollaro usando i sistemi infetti per generare cripto-valuta?

L'idea è venuta a **TA505**, un gruppo di pirati informatici specializzato in attacchi ad aziende operanti nel settore finanziario e commerciale. La nuova versione del loro **ServHelper**, un trojan che finora hanno utilizzato semplicemente per garantirsi l'accesso ai sistemi delle loro vittime, integra infatti un miner che viene installato automaticamente al momento dell'attacco.

Come si legge nel dettagliatissimo report pubblicato da **G Data**, si tratta di un malware estremamente complesso, che sfrutta numerose tecniche di offuscamento e una serie di procedure per evitare di essere rilevato da eventuali sandbox.

Il vettore di attacco usato dai pirati, spiegano i ricercatori, è normalmente un messaggio di posta elettronica che contiene un file **NSIS** (Nullsoft Scriptable Install System) la cui apertura avvia la procedura d'infezione.

Il malware, per prima cosa, si preoccupa di verificare di non

trovarsi in una sandbox virtuale. Per farlo, verifica in prima battuta la presenza di un file (**C:\aaa\_TouchMeNot\_.txt**) presente nelle istanze virtualizzate di Windows.

Solo a questo punto, il programma decodifica il modulo principale ServHelper e ne avvia l'esecuzione. Anche in questa seconda fase, però, viene eseguita una seconda verifica.

Questa volta il malware esegue un controllo di sistema attraverso **System Management BIOS** per ottenere informazioni sulle dimensioni della ROM e verificare che ammonti almeno a 2 MB.

Dal momento che non è presente alcuna ROM nei sistemi virtualizzati, a giudizio dei ricercatori l'operazione mira a verificare la presenza di indizi che indichino la presenza di un ambiente virtuale.

Se i controlli vanno a buon fine, ServHelper viene installato e, da questo momento, agisce come un servizio di controllo remoto, consentendo agli autori del malware un accesso completo al sistema.

Il modulo aggiuntivo, che i ricercatori hanno battezzato con il nome di **LoudMiner** a causa del fatto che fa un uso intensivo delle risorse di sistema, sfrutta una tecnica di offuscamento basata sulla virtualizzazione. Una volta installato nssm.exe (Non-Sucking Service Manager), uno strumento gratuito che consente di gestire i servizi su sistemi Windows, avvia una sessione di **VirtualBox** al cui interno “gira” il miner.

Risultato: oltre ad avere un accesso completo al sistema, i pirati di TA505 hanno da subito una rendita fissa sfruttando la potenza di calcolo dei sistemi compromessi.

Condividi l'articolo

---

Tsunami: il software di sicurezza targato Google diventa open

---

**Articoli correlati**

## Altro in questa categoria

---

[https://www.securityinfo.it/2020/07/13/servhelper-raddoppia-oltre-alla-backdoor-installare-un-miner/?utm\\_source=rss&utm\\_medium=rss&utm\\_campaign=servhelper-raddoppia-oltre-alla-backdoor-installare-un-miner](https://www.securityinfo.it/2020/07/13/servhelper-raddoppia-oltre-alla-backdoor-installare-un-miner/?utm_source=rss&utm_medium=rss&utm_campaign=servhelper-raddoppia-oltre-alla-backdoor-installare-un-miner)