nexthardware.com

a cura di: **Gian Paolo Collalto - giampa - 07-11-2014 13:30**

Attenti alla nuova Operazione Toohash

LINK (https://www.nexthardware.com/news/antivirus/6484/attenti-alla-nuova-operazione-toohash.htm)

G DATA segnala una nuova cyber campagna dall'Asia contro le aziende.

La maggior parte dei file scoperti proviene da Taiwan e da un'analisi dei documenti gli esperti di sicurezza ritengono che questo spyware sia stato utilizzato su obbiettivi situati anche in altre regioni della Cina.

Le soluzioni di sicurezza di G DATA hanno identificato il malware come Win32.Trojan.Cohhoc.A and Win32.Trojan.DirectsX.A.

"*Il malware negli allegati delle email sfrutta specificatamente una vulnerabilità in Microsoft Office e scarica un tool di accesso remoto sui computer infettati*", spiega Ralf Benzmà¼ller, Head of G↔ DATA SecurityLabs. "*In questa campagna abbiamo identificato due differenti tipologie di malware ed entrambe contengono noti componenti usati nel cyber spionaggio come moduli per l'esecuzione automatica di codici, file listing, furto di dati, ecc.*"

La console di amministrazione che i criminali usano per controllare i computer infetti è in parte in Cinese ed in parte in Inglese.

Un'analisi dettagliato di questo spyware è disponibile sul G DATA SecurityBlog (https://blog.gdatasoftware.com/blog/article/operation-toohash-how-targeted-attacks-work.html). (https://blog.gdatasoftware.com/blog/article/operation-toohash-how-targeted-attacks-work.html)