Facebook: si chiama Ramnit il virus all'attacco del social network

Data: 1 giugno 2012 | Autore: Redazione

LECCE, 06 GENNAIO 2012- Entra nei profili e invia spam ai contatti. Si chiama Ramnit il nuovo virus che ruba le password di facebook. Secondo gli esperti avrebbe sottratto le credenziali di accesso a 45 mila utenti nel Regno Unito e in Francia.[MORE]

Scoperto nel mese di aprile 2010, il Microsoft Malware Protection Center (MMPC) descrive Ramnit come "un multi-componente della famiglia di malware che infetta eseguibili di Windows così come i file HTML", "ruba informazioni sensibili come le credenziali FTP memorizzate e i cookie del browser". Usando questa backdoor, un aggressore remoto potrebbe istruire un computer infetto per eseguire azioni come scaricare un file ed eseguirlo o connettersi a un altro server e attendere istruzioni. Nel Report di luglio 2011 Symantec [PDF] ha stimato che varianti del worm Ramnit hanno rappresentato il 17,3 per cento di tutte le nuove infezioni da software dannosi.

Il worm si diffonde criptandosi e unendosi a file con estensione .DLL, .EXE e .HTML. Nell'agosto del 2011, Trusteer ha riferito che è Ramnit è diventato "finanziario". Dopo la fuoriuscita del codice sorgente di ZeuS a maggio, è stato suggerito che gli hacker dietro Ramnit hanno accorpato varie funzionalità di diffusione delle frodi finanziarie per creare una "creatura ibrida" che è ha le dimensioni e le capacità dell'infezione Ramnit e quelle finanziarie di data-sniffing di ZeuS. Il worm ha acquisito la capacità di iniettare il codice HTML in un browser Web, permettendo di bypassare a Ramnit l'autenticazione a due fattori e i sistemi di transazione a firme, ottenenendo l'accesso remoto alle

istituzioni finanziarie, le sessioni di online banking e penetrare in diverse reti aziendali dopo averle compromesse.

Con l'uso di un Sinkhole, Seculert ha scoperto che circa 800.000 computer sono stati infettati con Ramnit da settembre a fine dicembre 2011. Sembra, tuttavia, che questo non è l'ultima spirale. Recentemente, il laboratorio di ricerca Seculert ha identificato una variante finanziaria completamente nuova di Ramnit che mira a rubare le credenziali di login di Facebook.

Secondo Giovanni D'Agata, componente del Dipartimento Tematico Nazionale "Tutela del Consumatore" di Italia dei Valori e fondatore dello "Sportello dei Diritti" per proteggersi nel modo migliore dalle minacce, può essere utile informarsi sui rischi che si corre e possedere almeno una conoscenza di base sulle misure d'adottare.
Per esempio si consiglia di usare l' accortezza per evitare noie, quella di utilizzare password diverse per i vari network.
Inoltre si consiglia di adottare le seguenti misure per prevenire l'infezione del computer:
- Attivare un firewall sul computer.
- Ricevere gli ultimi aggiornamenti del computer per tutti i vostri software installati.
- Utilizzare un software antivirus aggiornato.
- Limitare i privilegi dell'utente del computer.
- Prestare attenzione quando si aprono gli allegati e di accettare trasferimenti di file.
- Prestare attenzione quando si clicca su link a pagine Web e Facebook
- Evitare di scaricare software pirata.
- Proteggersi da attacchi di social engineering.
- Utilizzare password complesse.

(notizia segnalata da **giovanni d'agata**)