TechCorner

# Nuovi attacchi, vecchi pericoli

**Dai ricercatori eScan un nuovo allarme contro messaggi di spam particolarmente nocivi**

30 Marzo 2010 - Il team di professionisti della sicurezza di **eScan** mette in guardia gli utenti di Internet dall'aprire email – nonché gli allegati – che abbiano per oggetto titoli quali *You have received A Hallmark E-Card!*, *Your friend invited you to twitter!*, *Thank you from Google!*, *Jessica would like to be your friend on hi5!* e *Shipping update for your Amazon.com order 254-71546325-658732*. In questo tipo di e-mail vengono infatti veicolati allegati zippati che contengono nuove versioni di malware nocivi.

Per esempio, l'e-mail che ha per oggetto *You have received A Hallmark E-Card!* viene diffusa con in allegato un postcard.zip (o altra dicitura simile). Il contenuto del file zip reca con sé dei malware che hanno un motore di mass mailing SMTP integrato per inviare email e che si diffondono attraverso la posta elettronica agli indirizzi raccolti nei sistemi infettati.

Il payload contiene anche un malware con le caratteristiche di Vundo (aka VirtuMonde/VirtuMundo), ovvero un trojan horse che scarica ed esegue file arbitrari potenzialmente malevoli da Internet. Vundo è in grado di infettare il sistema nel momento stesso in cui il browser apre il link a una pagina web, contenuto in una email spam. Il browser web viene infestato da popup pubblicitari e il virus riesce a gestire antivirus e i relativi programmi di sicurezza. Questo fastidioso trojan è molto insidioso perché, anche se viene rimosso il file che lo genera (virtumonde.dll), lo ricrea automaticamente. Infatti, la dll viene creata nella directory Windows system32 dall'avvio di Internet Explorer. E' inoltre in grado di iniettare il codice malevolo in processi legittimi, nel tentativo di nascondere la sua presenza nel sistema.

Esiste poi, un altro genere di mail nociva che sta girando nella rete e che sfrutta, per diffondersi, la popolarità dei social network quali Twitter e Hi5. Questi messaggi spam nascondono una variante di Buzus, un bot che si diffonde tramite il proprio motore di mass mailing SMTP. Buzus si diffonde copiando se stesso nei dischi rimuovibili e tenta di sottrarre informazioni riservate dal computer infettato. Questo tipo di trojan si configura, modificando il registro, per essere eseguito in modo automatico all'avvio del sistema.

I malware che vengono attualmente diffusi sono anche quelli che mostrano le diciture *Thank you from Google!* e " e che hanno in allegato attachment generalmente nominati Invitation Card.zip, Postcard.zip, Shipping documents.zip o CV-20100120-112.zip. Nel momento stesso in cui il malcapitato apre tali file, il sistema viene immediatamente infettato e il malware si attiva subito per tentare di infettare altri sistemi nel network inviando la stessa mail nociva agli indirizzi raccolti nei sistemi infettati.