FREEONLINE.it
La guida italiana alle risorse gratuite di Internet

# Lo staff di eScan mette in guardia gli utenti della rete dalla nuova ondata di attacchi spam

## *Diffuse in rete inedite versioni dei trojan Vundo e Buzus*

29/03/10 - 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 email vengono veicolati allegati zippati che contengono nuove versioni di malware nocivi.

Ad esempio, l'email 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 "Shipping update for your Amazon.com order 254-71546325-658732" 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.

"Una delle nostre maggiori premure è quella di rendere sempre più consapevoli gli utenti della rete sull'enorme rischio che corrono quando aprono email e allegati sospetti senza aver verificato l'autenticità del messaggio stesso - afferma Govind Rammurthy, CEO e Managing Director di MicroWorld - Le varianti dei malware si rivelano sempre più sofisticati rispetto alle precedenti versioni: hanno la capacità di compromettere il sistema in un secondo e di diffondere il virus all'intero network nel giro di un'ora. Per questo, noi di eScan non smetteremo mai di ribadire quanto sia importante avvalersi di un valido strumento per la protezione del PC nonché di avere

l'accortezza di mantenere sempre tale software aggiornato".

Per informazioni:
eScan
http://www.escanav.com

Laboratori Informatici
www.labinfo.it

About eScan

eScan è la soluzione di Real-Time Email e Webscanner per desktop e server, sviluppata e prodotta da MicroWorld. MicroWorld Winsock Layer (MWL) è la rivoluzionaria tecnologia che contraddistingue i prodotti eScan: ovvero un software di filtro per il quale passano tutti i contenuti delle comunicazioni via Internet bloccando i virus e le applicazioni che possono danneggiare l'utilizzazione del PC. Grazie all'utilizzo di tale tecnologia, eScan ha ottenuto numerose certificazioni e premi provenienti dalle più autorevoli fonti del settore quali: Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready, e Novell Ready.

La gamma di soluzioni MicroWorld per la Sicurezza Informatica, comprende: Escan, MailScan, X-Spam ed eConceal coprendo l'intero spettro dei requisiti di sicurezza. Il successo nello sviluppo di soluzioni innovative per le grandi, medie e piccole imprese, ISP e singoli utenti, ha reso MicroWold un saldo riferimento nel campo degli AntiVirus e sicurezza dati.

About Laboratori Informatici

Laboratori Informatici, società di sviluppo software e distribuzione prodotti per la sicurezza, nasce nel 1992 come società in grado di offrire soluzioni integrate e globali alle aziende che vogliano informatizzarsi o che desiderino rinnovare e potenziare la propria struttura informatica.
L'attività concentrata inizialmente sul territorio nazionale, si è ben presto allargata a paesi europei ed extraeuropei consentendo a Laboratori Informatici di entrare in contatto con aziende di rilevanza internazionale.
Una svolta importante nell'ambito delle attività di Laboratori Informatici si è verificata grazie all'accordo di distribuzione, in esclusiva, sul territorio nazionale dei prodotti della MicroWorld.

Laboratori Informatici – società del gruppo LMI - si presenta oggi sul mercato come azienda Leader di distribuzione.

TESTO PUBBLICATO DA
**Alessandro Esposito**
di Cast Adv & Communication