PER ULTERIORI INFORMAZIONI CONTATTARE:

Emanuela Lombardo
Symantec Italia
02/241151
emanuela_lombardo@symantec.com

Francesco Petrella – Nadia Lauria – Rosaria Callea
Pleon
02/0066290
francesco.petrella@pleon.com, nadia.lauria@pleon.com, rosaria.callea@pleon.com

Symantec pubblica l'Internet Security Threat Report XIV:l'Italia sale nelle classifiche EMEA dell'illegalità informatica

Nel 2008 l'Italia scala posizioni per numero di attività malevole registrate, per origine degli attacchi informatici e per numero di computer "bot infected".

A livello mondiale, le informazioni sottratte su carte di credito si confermano i più popolari "beni" in vendita nell'economia sommersa online (32% del totale), mentre lo spam su Internet è aumentato del 192%

Cupertino, Calif. - 14 aprile 2009 – Dai risultati dell'edizione numero XIV dell'Internet Security Threat Report di Symantec, pubblicato oggi, emerge che l'Italia scala posizioni nelle principali classifiche EMEA (Europa, Medio Oriente e Africa) sull'illegalità informatica. A influenzare le variazioni dell'Italia, tuttavia, contribuisce soprattutto la minore incidenza che i fenomeni registrati hanno avuto in altri Paesi rispetto al 2007.

In particolare, rispetto al 2007, l'Italia passa dal 5° al 4° posto per numero di attività malevole registrate, dal 7° al 5° tra i Paesi da cui hanno origine gli attacchi informatici e dal 4° al 3° per numero di computer "bot infected", ossia computer nei quali i cyber-criminali si sono insinuati per assumerne il controllo e usarli come "ponte" per lanciare attacchi informatici di vario tipo.

Il report, presentato su base annuale, analizza l'intero anno 2008. Lo studio raccoglie i dati provenienti da milioni di sensori Internet, ricerche e monitoraggio attivo delle comunicazioni degli hacker, e fornisce una panoramica globale dello stato attuale della sicurezza Internet. I dati contenuti nel report ISTR XIV sono stati raccolti nel periodo gennaio 2008-dicembre 2008.

I risultati globali

Dal Report emerge che gli Stati Uniti rimangono il Paese di origine di una larga parte delle attività informatiche malevole, attività che stanno registrando negli ultimi tempi un sensibile aumento anche in Paesi fino a oggi non associati a questo tipo di minacce.

Il report evidenzia anche come gli attacchi provenienti dal Web rimangano il principale vettore delle attività malevole su Internet, mentre gli attaccanti sono più che mai concentrati sul tentativo di conseguire guadagni economici dagli utenti finali colpiti. Lo studio pone in luce anche il fatto che l'economia sommersa non sembra aver risentito minimamente della crisi economica globale, ma appare più prospera e fiorente che mai.

Secondo il report, il Brasile (quinto nella graduatoria relativa al 2008 dall'ottavo posto del 2007), la Turchia (nona nel 2008 e quindicesima nel 2007) e la Polonia (decima, salita dal dodicesimo posto del 2007) vedono crescere le attività malevole in linea con lo sviluppo delle loro infrastrutture Internet e della popolazione di utenti broadband. Si prevede che i Paesi caratterizzati da infrastrutture Internet relativamente recenti e in via di sviluppo registreranno livelli

crescenti di attività malevole fino a quando non verranno rafforzate le misure di sicurezza atte a contrastarle.

Nel 2008 l'incidenza delle attività malevole è diminuita negli Stati Uniti (23% dal 26% del 2007), in Cina (9% contro l'11% del 2007) e in Germania (6% anziché 7%). Questi Paesi possiedono estese infrastrutture broadband in costante sviluppo che costituiscono bersagli invitanti per gli attaccanti.

Come è accaduto nel 2007, le attività pericolose condotte nel 2008 hanno avuto il Web quale principale canale di provenienza, in parte a causa della crescente sofisticazione e proliferazione delle infrastrutture Internet e in parte per il loro crescente uso in molteplici attività. L'accessibilità delle applicazioni Web, unitamente alle onnipresenti vulnerabilità facilmente sfruttabili che le caratterizzano, ha contribuito anch'essa alla diffusione delle minacce Web durante lo scorso anno. Di tutte le vulnerabilità identificate nel 2008, il 63% riguardava le applicazioni Web, in salita dal 59% del 2007. Inoltre, mentre nel 2008 sono state identificate 12.885 vulnerabilità XSS (Cross-Site Scripting) specifiche di determinati siti, soltanto il 3% (394) di esse è stato accompagnato dal rilascio di apposite patch. Il report ha evidenziato anche come gli attacchi Web abbiano origine in tutto il mondo, in modo particolare da parte di Stati Uniti (38%), Cina (13%) e Ucraina (12%). Tuttavia, sei dei primi dieci Paesi di origine delle minacce Web appartengono all'area Europa-Medio Oriente, per un totale del 45%, un valore superiore a ogni altra regione.

Lo studio sottolinea anche come gli attaccanti siano impegnati a sottrarre le informazioni relative agli utenti finali. Nel 2008 il 78% delle minacce indirizzate al furto di informazioni riservate si è concretizzato nella sottrazione di dati relativi agli utenti, contro il 74% del 2007. Questo tipo di minacce si rivela particolarmente utile per i criminali informatici, in quanto i dati sottratti possono essere proficuamente utilizzati per rubare l'identità degli utenti o quale ausilio per ulteriori attacchi. Le minacce associate a logging di tastiera, utilizzati per sottrarre informazioni come i dati relativi ai conti correnti bancari, hanno sommato il 76% degli attacchi rivolti alle informazioni riservate, in crescita dal 72% del 2007. Il 76% dei tentativi di phishing, inoltre, ha avuto quale bersaglio società operanti nel settore dei servizi finanziari, il quale è risultato il più esposto alle violazioni delle identità proprio a causa dei furti di dati. Con il 44% degli utenti Internet negli Stati Uniti, il 64% in Canada e il 46% in Francia impegnati nel condurre attività di online banking che possono richiedere la digitazione di informazioni relative a carte di credito o credenziali bancarie, non sorprende che la maggioranza delle attività di phishing abbia quale bersaglio società operanti in questo settore. In linea con questa tendenza, il 12% di tutte le fughe di dati registrate nel 2008 ha riguardato informazioni relative a carte di credito.

Analizzando i dati contenuti nel suo ultimo report sull'economia sommersa online, Symantec ha rilevato che quest'ultima è più florida che mai. Per esempio, le carte di credito con bande magnetiche vergini possono essere prodotte in un certo Paese, inviate in un secondo Paese per la copia delle informazioni rubate, e quindi spedite nei Paesi di origine dei dati sottratti. Le organizzazioni criminali specializzate nella distribuzione di codici malevoli e nella gestione di siti Web malevoli hanno riscosso un tale successo da essere accreditate di quasi la metà degli attacchi di phishing verificatisi in tutto il mondo nel 2008. L'economia sommersa ha visto la nascita di vere e proprie pseudo - aziende specializzate nello sviluppo su larga scala di codice pericoloso, strutturate in maniera simile alle società produttrici di software legittimo. L'economia sommersa, inoltre, è quanto mai prospera: lo dimostra il fatto che, mentre nel mercato legittimo i prezzi sono in calo, nell'economia sommersa essi sono rimasti costanti dal 2007 al 2008.

Dati principali

- Nel 2008 Symantec ha identificato in tutto il mondo oltre 1,6 milioni di nuove minacce. Si tratta del 60% circa dei 2,6 milioni di esemplari di codice pericoloso rilevati dalla società in 27 anni.
- Nel corso del 2008 è stato rilevato complessivamente un totale di 55.389 host di phishing, con un aumento del 66% rispetto al 2007, anno in cui il numero ammontava a 33.428.
- Le informazioni relative alle carte di credito hanno costituito il prodotto più pubblicizzato sui server dell'economia sommersa monitorati da Symantec, pesando per il 32% di tutti i prodotti e i servizi offerti; un incremento sostanziale rispetto al 21% del 2007.
- Symantec ha registrato un aumento del 192% nello spam su Internet, passando dai 119,6 miliardi di messaggi del 2007 ai 349,6 miliardi del 2008. Nel 2008 le reti botnet sono state la causa della diffusione del 90% delle mail di spam.
- Entro la fine del 2008 i computer infettati dal worm Downadup Conflicker assommavano a oltre 1 milione. Questo worm è stato in grado di diffondersi con estrema rapidità grazie ai sofisticati meccanismi di propagazione utilizzati e alla capacità di trasmettersi attraverso i supporti rimovibili. Nel primo trimestre del 2009 sono saliti a oltre 3 milioni i computer infettati dal worm Downadup Conflicker.

LINK UTILI

- Symantec Internet Security Threat Report XIV Microsite
- Symantec Internet Security Threat Report XIV Flash Demo
- Symantec Internet Security Threat Report XIV Webcast:
- Symantec Internet Security Report XIV Podcast
- Symantec Report on the Underground Economy
- Symantec Web-Based Attacks White Paper
- Symantec is Security

Informazioni sull'Internet Security Threat Report

Symantec Internet Security Threat Report propone analisi e approfondimenti sulle attività delle minacce, una panoramica delle vulnerabilità conosciute e le principali caratteristiche del codice pericoloso. Tratta inoltre le tendenze inerenti il phishing e lo spam, e osserva le attività condotte dai server dell'economia sommersa.
Symantec dispone di una delle fonti di informazioni di dati più estese a livello mondiale. Il Symantec Global Intelligence Network reperisce infatti i dati sulla sicurezza da oltre 240.000 sensori che monitorano costantemente le attività della Rete in oltre 200 Paesi, attraverso le soluzioni e i servizi Symantec quali Symantec DeepSight™ Threat Management, System e Symantec™ Managed Security Services e i prodotti Norton, oltre che da fonti terze parti. Oltre 123 milioni di client, server e sistemi gateway sui quali sono stati installati i prodotti antivirus Symantec sono fonte di dati e informazioni su codice pericoloso. Una rete di raccolta che riceve dati da tutto il mondo acquisendo minacce e attacchi completamente nuovi e fornendo un'analisi approfondita dei metodi utilizzati dagli attaccanti. Symantec fornisce uno dei database più completi al mondo in fatto di vulnerabilità; quelle attualmente registrate ammontano a oltre 32.000 (coprendo circa due decenni di attività) e hanno colpito oltre 72.000 tecnologie di più di 11.000 vendor. Un altro strumento utilizzato da Symantec è la mailing list BugTraq, uno dei forum più popolari con circa 50.000 iscritti che su base quotidiana scambiano informazioni e segnalazioni sulle vulnerabilità della Rete.
I dati relativi a spam e del phishing vengono acquisiti da fonti diverse come Symantec Probe Network, una rete di oltre 2,5 milioni di trappole; MessageLabs Intelligence, una fonte di informazioni e di analisi di problematiche, tendenze e statistiche inerenti la sicurezza della messaggistica; e altre tecnologie Symantec. I dati raccolti provengono da più di 86 Paesi di tutto il mondo. Ogni giorno vengono esaminati i dati provenienti da 16 datacenter, ovvero oltre otto miliardi di messaggio email e più di un miliardo di richieste Web. Symantec raccoglie infine i dati attraverso un'ampia comunità antifrode di aziende, vendor di sicurezza e più di 50 milioni di consumatori.
L'insieme di questi strumenti offre agli analisti Symantec una fonte di dati senza paragoni grazie alla quale è possibile identificare, analizzare e commentare le tendenze emergenti negli attacchi, nel codice pericoloso, nel phishing e nello spam. Symantec Internet Security Threat Report fornisce così ad aziende e consumatori le informazioni necessarie a mettere in sicurezza sistemi e infrastrutture oggi così come in futuro.

Informazioni su Symantec

Symantec è il leader globale nella creazione di soluzioni per la sicurezza, lo storage e la gestione dei sistemi in grado di aiutare aziende e consumatori a proteggere e gestire le informazioni. I nostri software e servizi proteggono da un numero maggiore di rischi e in diverse situazioni, in modo più completo ed efficiente, per una maggiore fiducia dell'utente ovunque siano usati o archiviati dati.

Per ulteriori informazioni, consultare il sito web all'indirizzo www.symantec.com o www.symantec.it

###

NOTE PER GLI EDITORI: Per maggiori informazioni riguardo Symantec Corporation e i suoi prodotti è possibile visitare la Symantec News Room all'indirizzo http://www.symantec.com/news.