PER ULTERIORI INFORMAZIONI CONTATTARE:

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

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

Uno studio Symantec svela come i cybercriminali convincono gli utenti ad acquistare soluzioni di sicurezza fasulle

Per i contraffattori guadagni superiori allo stipendio di Barack Obama

CUPERTINO, Calif. – 28 ottobre 2009 - Symantec Corp. (Nasdaq: SYMC) ha presentato i risultati del suo nuovo studio dal titolo “Report on Rogue Security Software”. Basandosi sui dati raccolti nel periodo fra luglio 2008 e giugno 2009, Symantec ha messo in luce come i cybercriminali si stiano sempre più servendo di tattiche di persuasione online fondate sulla paura per convincere gli utenti ad acquistare soluzioni di sicurezza contraffatte. Questo tipo di software, detto anche “scareware”, appare, infatti, come legittimo, mentre in realtà si tratta di applicazioni fasulle che non forniscono alcun servizio di tutela della sicurezza. Al contrario, spesso questi software hanno come obiettivo quello di installare dei codici maligni di compromettere la sicurezza generale della macchina.

Per incoraggiare gli ignari utenti a installare queste finte soluzioni, i cybercriminali pubblicano dei veri e propri banner finalizzati a fomentare timori e ansie in fatto di minacce alla sicurezza. Queste pubblicità in genere recitano affermazioni ingannevoli, come ad esempio "se vedete lampeggiare questo banner è probabile che il vostro computer sia a rischio o già infetto”. In questo modo l'utente prova un senso di urgenza e viene spinto a seguire il link per far analizzare la propria macchina o scaricare il software che consente di eliminare la presunta minaccia. Secondo lo studio, il 93% delle installazioni software derivanti dai 50 principali programmi di questo tipo è stato intenzionalmente scaricato dallo stesso utente. Fino a giugno 2009, Symantec ha rilevato oltre 250 diversi finti programmi per la sicurezza.

Inizialmente la perdita economica per l'utente che si lascia trascinare in questo genere di truffa va da un minimo di 30 a un massimo di 100 dollari; però il prezzo da pagare per riacquistare l'identità violata potrebbe risultare significativamente superiore. Infatti, questi programmi contraffatti non solo costano denaro, ma sfruttano e sottraggono i dati sensibili forniti durante la fase di acquisto per perpetrare ulteriori frodi, o rivenderli sul mercato sommerso delle informazioni dando vita a un vero e proprio furto di identità.

A peggiorare ulteriormente il quadro, l'esistenza di software contraffatti progettati appositamente per installare codici maligni che mettono gli utenti a rischio di attacco da ulteriori minacce. Di conseguenza, installare questo tipo di programmi può portare a una seria diminuzione del livello di sicurezza di un computer proprio quando, al contrario, l'utente è convinto di rafforzarne la capacità di difesa. Ad esempio, i programmi fasulli sono in grado di dare all'utente una serie di istruzioni affinché questi riduca o disabiliti qualsiasi settaggio di sicurezza mentre registra questo software-truffa, piuttosto che di impedire l'accesso a siti Web legittimi specializzati in soluzioni di sicurezza successivamente

all'installazione. Paradossalmente, gli utenti vengono pertanto esposti alle minacce che il software contraffatto promette proprio di contrastare.

Messaggi pubblicitari ingannevoli puntano sulla paura per far sì che gli utenti acquistino applicazioni fasulle

Sono diversi i metodi utilizzati per trarre in inganno gli utenti e convincerli a scaricare applicazioni fasulle; e molti di essi si basano su tattiche che fanno leva sulla paura e su altri escamotage di social engineering. Il software di sicurezza fasullo viene pubblicizzato secondo le modalità più diverse, inclusi siti Web sia pericolosi sia legittimi quali blog, forum, siti di social networking e siti per adulti. Anche se i siti legittimi non sono parte attiva di queste truffe, essi possono subire una violazione e pubblicizzare quindi queste finte applicazioni. I siti di software di sicurezza fasulli possono anche apparire in cima alla lista degli esiti prodotti da un motore di ricerca se gli ideatori della truffa sono intervenuti per manipolare i risultati.

Per incrementare i margini di successo di questo genere di operazioni, i creatori di software falsi progettano i loro programmi rendendoli il più possibile credibili imitando in tutto e per tutto quelli veri. Bisogna inoltre evidenziare che questi programmi spesso vengono distribuiti su siti Web che appaiono totalmente affidabili e credibili, e che agevolano l'utente a scaricare il software in questione. Alcuni siti pericolosi si servono di servizi di pagamento online legali per eseguire le transazioni con carte di credito mentre altri inviano una mail all’ignara vittima con una ricevuta di acquisto – completa di numero di serie e numero di telefono del servizio clienti.

Intermediari distribuiscono software contraffatto per aggiudicarsi premi o guadagni

I cybercriminali stanno traendo vantaggio da un modello di business altamente organizzato basato sul concetto pay-for-performance, un approccio in base al quale i truffatori vengono pagati per ingannare gli utenti e far installare loro finti programmi di sicurezza. Secondo quanto emerso dallo studio, i primi dieci affiliati a TrafficConverter.biz, sito che distribuisce applicazioni contraffatte, avrebbero guadagnato una media di 23.000 dollari a settimana durante i dodici mesi presi in esame dalla ricerca, ovvero una cifra equivalente a tre volte lo stipendio del Presidente degli Stati Uniti (1).

Queste pratiche sono del tutto simili a quelle utilizzate nei programmi marketing basati su affiliazione utilizzati dai normali retailer online. Queste iniziative ricompensano i partecipanti sulla base del numero di visitatori condotti al sito Web del retailer grazie alle capacità e agli sforzi di marketing compiuti dall'affiliato. Attraverso questo modello gli affiliati che prendono parte alle truffe in questione arrivano a guadagnare cifre comprese fra 0,01 e 0,55 dollari per ciascuna installazione andata a buon fine. La classifica dei prezzi più elevati vede in testa le installazioni effettuate dagli utenti di Stati Uniti, seguiti da Regno Unito, Canada e Australia. Alcuni siti di distribuzione offrono ai loro affiliati anche degli incentivi erogati sotto forma di bonus per un determinato numero di installazioni, oltre a punti e premi VIP come auto di lusso o prodotti di elettronica.

I consigli di Symantec a riguardo sono rivolti alle aziende e agli utenti individuali, invitati a utilizzare sempre le più recenti soluzioni per la protezione dai rischi legati alla sicurezza come ad esempio Symantec Endpoint Protection o Norton Internet Security. Gli utenti e le imprese sono inoltre chiamati a utilizzare le best practice disponibili per la protezione e la mitigazione, presentate nell'allegato A dello studio Report on Rogue Security Software. In particolare,

gli utenti privati dovrebbero acquistare e installare solo software collaudati e forniti da produttori di sicurezza affidabili, le cui soluzioni vengono vendute presso punti vendita sicuri sul territorio oppure online. Le best practice per la protezione e la mitigazione includono:

- Evitare di seguire i link contenuti in email, in quanto potenziali connessioni con siti Web violati o pericolosi. Al contrario, digitare manualmente l'URL del sito Web legittimo conosciuto.
- Mai visualizzare, aprire o eseguire gli allegati della posta elettronica a meno che siano attesi e provengano da una fonte fidata. Diffidare di qualsiasi email che non sia direttamente destinata al vostro indirizzo di posta.
- Prestare la massima attenzione alle finestre pop-up e ai banner pubblicitari che imitano nomi legittimi. I messaggi di errore sospetto che appaiono all'interno del browser Web spesso nascondono truffe finalizzate a fare in modo che l'utente scarichi e installi il prodotto fasullo.

Fonti consultabili:

Pausa e ansia, ecco come convincere gli utenti ad acquistare software di sicurezza fasulli. www.symantec.com/xxxx
Il software di sicurezza contraffatto comunica agli utenti un finto senso di sicurezza, esponendoli invece a rischi ben maggiori www.symantec.com/xxxx
Ingannare gli utenti regala ai cybercriminali stipendi mensili a sei cifre. www.symantec.com/xxxx
Symantec spiega come individuare e difendersi dai software di sicurezza fasulli. www.symantec.com/xxx

Dichiarazioni a supporto

“I risultati dello studio Report on Rogue Security Software dimostrano chiaramente come i cybercriminali siano ben preparati e agguerriti nei confronti degli utenti che oggi navigano su Internet”, ha spiegato Stephen Trilling, Senior Vice President, Symantec Security Technology and Response. “Per evitare di cadere nelle loro trappole, Symantec consiglia vivamente di assicurarsi sempre di utilizzare le ultimissime versioni dei software di protezione acquistandole direttamente sui siti Web dei vendor di fiducia”.

“I creatori di scareware hanno tutte le capacità e gli strumenti per truffare migliaia di persone, sottraendo piccole somme contemporaneamente riuscendo così a guadagnare forti cifre aggregate", ha dichiarato David Wall, PhD. Professor Centre for Criminal Justice Studies, University of Leeds. “Questo genere di frode funziona bene perché fa leva sulla psicologia dell'utente, il quale è portato a pensare di essere la vittima imminente di una minaccia che solo il finto software proposto è in grado di debellare. In realtà si tratta di una vera e propria fregatura. Il mio consiglio è quello di essere molto cauti quando si naviga online e scaricare solo da fonti fidate".

Ulteriori informazioni

- Le prime cinque applicazioni-truffa segnalate sono SpywareGuard 2008, AntiVirus 2008, AntiVirus 2009, SpywareSecure e XP AntiVirus.
- Sui i vari siti di distribuzione esaminati da Symantec, gli affiliati vengono pagati 0,55 dollari per le installazioni di questi software eseguiti da utenti residenti negli Stati Uniti, 0,52 dollari per quelli di Regno Unito e Canada, e 0,50 dollari per gli utenti australiani.

    - Il quinto posto nella classifica dei prezzi pagati agli affiliati è significativamente inferiore, ovvero 0,16 dollari per le installazioni eseguite in Spagna, Irlanda, Francia e Italia.
    - Le differenze di prezzo per installazione da Paese a Paese dipendono dal livello di probabilità che gli utenti di quella determinata nazione siano disposti a pagare per l'applicazione fasulla.
- Il 93% dei programmi falsi viene pubblicizzato attraverso un sito Web appositamente sviluppato per questo scopo; il 52% viene promosso tramite pubblicità Internet.
- Delle prime 50 applicazioni fasulle segnalate da Symantec fra luglio e giugno 2009, il 61% riguarda il Nordamerica; il 31% la regione Europa, Medio Oriente e Africa; il 6% la zona Asia/Pacifico-Giappone; e il 2% l'area dell'America Latina.
    - Le percentuali più elevate riguardanti Nordamerica ed EMEA trovano giustificazione nel fatto che la maggior parte delle attività pericolose si verifica proprio in queste due regioni.
    - In particolare, la preponderanza del Nordamerica è data anche dal fatto che gli affiliati sono pagati molto di più in base alle singole installazioni quando nella truffa cadono gli utenti di questo Paese.

Fonti aggiuntive

Click to Tweet: Questo tipo di truffa porta agli affiliati stipendi a sei cifre. www.symantec.com/xxxx
Click to Tweet: @Symantec svela i nomi dei primi cinque programmi fasulli. www.symantec.com/xxxx
Click to Tweet: @Symantec spiega come individuare e reagire al software fasullo. www.symantec.com/xxx

Maggiori informazioni sono disponibili all'interno della nostra cartella stampa online
Accesso alla presentazione su Slideshare.net
Consultazione della mappa di distribuzione globale dei server di software di sicurezza fasulli
Download di esempi infografici dettagliati inerenti ai guadagni degli affiliati
Consultazione della Symantec Guide to Scary Internet Stuff on Misleading Applications
Link a video e podcast Symantec

Informazioni sullo studio

Symantec Report on Rogue Security Software, stilato in collaborazione con la Security Technology and Response (STAR), è un'analisi approfondita delle applicazioni di sicurezza false. Il report include una panoramica su come questi programmi operano e danneggiano gli utenti, prendendo in esame anche le implicazioni di rischio, i diversi metodi di distribuzione e i nuovi vettori utilizzati negli attacchi. Lo studio prevede inoltre una breve presentazione delle truffe più rilevanti e una valutazione sulle zone geografiche nelle quali questo genere di minacce è più frequente. Infine, lo studio riporta una riflessione sul numero di server osservati da Symantec che ospitano questo genere di truffe. Salvo specifiche diverse, il periodo preso in esame dallo studio è compreso fra il 1' luglio 2008 e il 30 giugno 2009.

Security Technology and Response

La struttura Security Technology and Response (STAR), che include anche Security Response, è un team mondiale di ingegneri specializzati in sicurezza, analisti di minacce e ricercatori che fornisce competenze in tema di funzionalità, contenuti e minacce basandosi sull'offerta di prodotti Symantec per la sicurezza aziendale e consumer. Potendo contare

su diversi centri globali di risposta situati in ogni parte del globo, STAR monitora i report di codici maligni provenienti da oltre 130 milioni di sistemi collegati a Internet ricevendo dati da più di 240.000 sensori di rete posizionati in oltre 200 Paesi, e tracciando più di 32.000 vulnerabilità destinate a ben 72.000 tecnologie di oltre 11.000 vendor. Il team sfrutta questa ampia base di informazioni per sviluppare e offrire la più elevata e completa protezione di sicurezza possibile.

Le soluzioni di sicurezza di Symantec

Symantec aiuta le aziende a mettere in sicurezza e gestire le loro infrastrutture di sicurezza globali basate sulle informazioni, i loro sistemi di sicurezza endpoint e le loro soluzioni di sicurezza per la messaggistica e le applicazioni.

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.