GFI Labs
Uncovering the latest online threats

I falsi antivirus tornano ad attaccare aziende e utenti

Rilevata in Febbraio una recrudescenza nella diffusione di falsi programmi antivirus spesso distribuiti tramite spam che include l'exploit Blackhole.

Milano, 16 Marzo 2012 – GFI Software ha reso disponibile il **VIPRE® Report**, la classifica delle prime 10 minacce informatiche, rilevate nel mese di Febbraio 2012. In particolare, i GFI Labs hanno fornito informazioni, attraverso il Malware Protection Center blog, su una nuova ondata di falsi programmi antivirus (o Rogue AV). Questo fenomeno, in crescita dall'inizio dell'anno, ha registrato un picco il mese scorso nelle nuove varianti degli antivirus fasulli.

"Nonostante la velocità di diffusione degli antivirus fasulli sia rallentata alla fine dello scorso anno, stiamo assistendo ad una loro recrudescenza e, in ogni caso, questa rimane una delle tecniche più utilizzate dai criminali informatici", ha affermato Chris Boyd di GFI Software, analista senior per i rischi informatici. "Gli utenti non devono assolutamente abbassare la guardia. E' necessario valutare sempre e attentamente qualsiasi tipo di software che sembri aver infettato il PC (anche se sembra autentico) che richieda un numero di carta di credito o la condivisione di dati sensibili, soprattutto se si tratta di un software che non è stato installato né da voi né dai vostri dipendenti".

Molti programmi antivirus fasulli vengono inviati attraverso mail di spam contenenti link dannosi all'exploit Blackhole - uno strumento utilizzato dai criminali informatici per individuare le vulnerabilità non ancora coperte da patch all'interno di applicazioni software di aziende leader di mercato come Microsoft e Adobe. Gli utenti infettati da tale minaccia vengono reindirizzati verso siti illeciti dove il loro sistema viene colpito da programmi che, solo in apparenza, eseguono una scansione del PC oppure che contengono avvisi riguardanti virus e altre opzioni di sicurezza per il PC inesistenti; in questo modo, gli utenti vengono indotti ad inviare i dati della loro carta di credito per acquistare delle protezioni che non esistono.

Questi programmi, per non essere individuati, vengono costantemente modificati, con l'introduzione di nuove varianti in grado di propagarsi ogni 12 - 24 ore. Quando si trovano di fronte ad un possibile antivirus fasullo, gli utenti possono visitare il Malware Protection Center per ricevere suggerimenti su come rimuoverlo oppure scaricare il tool gratuito per la rimozione dei virus, **VIPRE® Rescue** di GFI Software.

Festività, tasse e giochi online: così colpiscono i criminali informatici

Il mese scorso sono stati rilevati episodi di phishing nei quali i criminali informatici si sono spacciati per rappresentanti di Intuit Inc., un'importante azienda statunitense proprietaria di TurboTax®, un programma molto diffuso ed utilizzato per l'elaborazione delle tasse. Alle vittime veniva richiesta una verifica dei dati fiscali perché, si segnalava nella mail, erano state riscontrate alcune discrepanze con le informazioni in possesso della Social Security Administration; con questo trucco venivano invece condotte verso un sito Blackhole.

Nel frattempo, un falso account dell' American Institute of Certified Public Accounts inviava delle email nelle quali si citava un "accertamento relativo ad una falsa dichiarazione dei redditi", in modo da spaventare le vittime e indurle ad aprire allegati all'apparenza innocui ma, invece, estremamente pericolosi.

Sempre il mese scorso, un ben più tradizionale attacco del crimine informatico diretto agli utenti di Tumblr, prometteva un buono omaggio di Victoria's Secret del valore di 500 dollari. Come per precedenti attacchi spam, in cui venivano offerti buoni omaggio di Starbucks e biglietti aerei gratuiti, i post di Tumblr sembravano autentici perché il mittente da cui provenivano era un fantomatico - ma realistico -"Tumblr Staff Blog." Quando gli utenti cliccavano su questi link veniva loro richiesto di iscriversi a varie promozioni e di inviare i loro dati, in modo da poter ricevere il buono omaggio.

I criminali informatici hanno inoltre colpito i giocatori online, attraverso alcuni video di YouTube, che li incoraggiavano a scaricare un programma in grado di generare alcuni codici per ottenere punti gratuiti Microsoft (la valuta utilizzata nel marketplace Xbox LIVE®). Questo programma induceva poi l'utente a compilare numerosi moduli con i suoi dati personali, promettendo in cambio le password necessarie per la creazione dei codici.

Le 10 minacce principali rilevate nel mese di Febbraio
L'elenco delle 10 minacce principali di GFI Software è stato stilato analizzando le segnalazioni provenienti dalle decine di migliaia di utenti dell'antivirus GFI VIPRE, che fanno parte del sistema di rilevazione automatico delle minacce **GFI ThreatNet™.** Le statistiche di ThreatNet indicano come i trojan rappresentino ancora la maggiore minaccia, dominando le prime posizioni della classifica di Febbraio.

Nome del virus	Tipologia	Percentuale
Trojan.Win32.Generic	Trojan	35.63
GamePlayLabs	Browser Plug-in	3.66
Yontoo	Adware	2.79
INF.Autorun (v)	Trojan	1.41
Trojan.Win32.Ramnit.c (v)	Trojan	1.02
Trojan-Spy.Win32.Zbot.gen	Trojan	0.94
Virus.Win32.Sality.at (v)	Virus.W32	0.94
Worm.Win32.Downad.Gen (v)	Worm.W32	0.92
Trojan.Win32.Jpgiframe (v)	Trojan	0.87
GameVance	Adware (General)	0.87

GFI Labs

I GFI Labs sono specializzati nella scoperta e analisi delle vulnerabilità e dei malware pericolosi, che potrebbero essere sfruttati per attacchi via Internet ed e-mail. Il team di ricerca indaga attivamente sui nuovi attacchi malware, creando e testando nuove risorse per i prodotti VIPRE home e business.

GFI

GFI Software rappresenta la migliore fonte di software per la protezione web e della posta elettronica, archiviazione e fax, networking e software di sicurezza, nonché di soluzioni IT hosted per le piccole e medie aziende, commercializzati attraverso un'estesa comunità di partner. I prodotti GFI sono disponibili on-premise, nella 'nuvola' o in modalità mista. Grazie alla tecnologia vincitrice di numerosi riconoscimenti, a una politica tariffaria aggressiva e alla particolare attenzione rivolta alle esigenze specifiche delle piccole e medie aziende, GFI Software è in grado di soddisfare le esigenze delle PMI su scala mondiale. Come fornitore di infrastrutture per le PMI, GFI ha uffici negli Stati Uniti, Regno Unito, Austria, Australia, Malta, Hong Kong, Filippine e Romania, a supporto di centinaia di migliaia di installazioni in tutto il mondo. GFI Software è un'azienda orientata alla collaborazione con il canale e si avvale infatti di migliaia di partner in tutto il mondo. Inoltre è un Microsoft Gold ISV Partner.

Ufficio Stampa:

GFI
David Kelleher: dkelleher@gfi.com
GFI - Malta: Tel: +356 2205 2000
www.gfi.com

Prima Pagina Comunicazione
Stefania Scroglieri
Tel: 02/76.11.83.01
email: stefania@primapagina.it