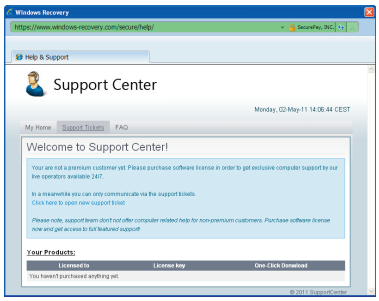
FraudTool: virus/malware che si spacciano per antivirus...

...per indurre l'utente ad acquistarli e impossessarsi così del numero della carta di credito. La risposta di TG Soft.

I FraudTool, letteralmente Tool Fraudolenti, sono software realizzati ad arte per presentarsi come software antivirus, e spaventare l'utente con segnalazioni allarmanti riguardanti la sicurezza del suo computer per indurlo ad acquistare una ipotetica versione a pagamento per risolvere le infezioni inesistenti. Ovviamente tale versione a pagamento non esiste e si rivela poi solo un espediente per impossessarsi dei dati della carta di credito del malcapitato utente.
Di questi FraudTool ve ne sono in circolazione numerosissime varianti. Spesso hanno interfacce grafiche simili o addirittura uguali, studiate ad arte per essere accattivanti e credibili, in modo da guadagnarsi la fiducia degli inconsapevoli utenti. Si insinuano nel computer durante la navigazione in Internet oppure invogliando l'utente a cliccare su immagini che rappresentano finti messaggi o domande, camuffati per sembrare messaggi di sistema. Una volta avviati fingono di eseguire una scansione del computer, che immancabilmente segnala la presenza di un numero elevato di virus/malware. Ovviamente promettono anche che tutti i virus/malware saranno debellati con l'acquisto di una versione completa dell'antivirus in questione.
I FraudTool hanno due obiettivi principali: indurre l'ignaro utente all'acquisto immediato del teorico software, per cifre generalmente non molto elevate ($ 10-20), ma soprattutto carpire dati della carta di credito per poi utilizzarli in proprio o cederli a organizzazioni dedicate ad acquisti sul web (almeno fino a quando la carta non verrà bloccata).
È chiaro che l'utilizzo della carta di credito per l'acquisto di un software di cui non si ha alcuna conoscenza, e del quale non sia nota e rintracciabile la software house produttrice, è assolutamente da evitare.
Ovviamente per gli autori di questi malware è di particolare interesse mantenere la loro creazione difficilmente intercettabile dai vari software antivirus disponibili sul mercato. Quindi, per far sì che non siano intercettati, i file portatori vengono modificati ad arte anche più volte nello stesso giorno.
A volte l'utente che rimane vittima di questo raggiro evita di sporgere denuncia alla polizia postale poiché la 'piccola' cifra che ha pagato e la vergogna per essere caduto in questo inganno lo fanno desistere dal segnalare alle autorità competenti la truffa. Quindi si limitano a bloccare la propria carta di credito.
Purtroppo gli autori di questi FraudTool, visti gli interessi economici in gioco, sono dei virus-writer professionisti e sono quindi impegnati a diffondere nuove varianti dei file portatori con frequenza sempre maggiore. In questo modo, non appena un antivirus abbia provveduto a mettere a punto l'aggiornamento per la sua univoca identificazione e rimozione, il FraudTool stesso e i malware a questo associati procedono ad auto-aggiornarsi di modo da rendersi nuovamente invisibili all'antivirus, così che quest'ultimo non riesca a identificarli e rimuoverli almeno per quel breve periodo di tempo, fino al successivo aggiornamento, che intanto garantisce ai virus writer di guadagnare con il loro operato.
Esempi di FraudTool realmente circolanti, come il recente Windows Recovery, si possono trovare nel blog del C.R.A.M. (Centro Ricerche



AntiMalware di TG Soft) collegandosi al sito www.malwarelist.org.

Come difendersi

La suite AntiVirus e AntiMalware Vir.IT eXplorer PRO di TG Soft, oltre a essere costantemente aggiornata con particolare attenzione ai virus/malware realmente circolanti, integra nello scudo residente la tecnologia proprietaria Intrusion Detection. Tale tecnologia si basa su un approccio euristico e permette di segnalare in tempo reale le intrusioni dei virus/malware di nuova generazione – non ancora identificati dagli antivirus – che si pongono in esecuzione automatica, con l'opportunità di inviarli gratuitamente al C.R.A.M. per l'analisi e l'eventuale aggiornamento della suite. Inoltre i clienti che dovessero incontrare questi agenti malware possono godere del supporto telefonico e online dei ricercatori del C.R.A.M., in modo da evitare di cadere nel tranello dell'incauto acquisto con carta di credito.
Per toccare con mano le potenzialità della suite Vir.IT eXplorer PRO, TG Soft rende disponibile gratuitamente Vir.IT eXplorer Lite – Free Edition – che, oltre a essere liberamente utilizzabile sia in ambito privato che aziendale senza violazione di licenza, è interoperabile con eventuali altri AntiVirus e/o Internet Security, sia commerciali che gratuiti, presenti nel computer senza provocare rallentamenti o conflitti. Vir.IT eXplorer Lite agisce da antivirus integrativo e permette di avere non solo un controllo incrociato grazie alle scansioni manuali o schedulate/programmate, ma mette a disposizione una sentinella pronta a segnalare eventuali intrusioni da parte di virus/malware di nuova generazione che si pongono in esecuzione automatica, grazie alla tecnologia proprietaria Intrusion Detection integrata. Questa stessa tecnologia dà l'opportunità di inviare gratuitamente al C.R.A.M. i file segnalati come sospetti portatori di virus/malware di nuova generazione, per l'analisi e l'aggiornamento del software.

www.tgsoft.it

A.C.R.

VCE nomina Magirus distributore autorizzato EMEA

Avrà il compito di portare sul mercato europeo le soluzioni Vblock Infrastructure Platform, basate su tecnologia Cisco, EMC e Vmware.

Le piattaforme per la virtualizzazione Vblock saranno distribuite da Magirus a livello europeo. Virtual Computing Environment (VCE) ha scelto proprio Magirus come primo distributore autorizzato per le competenze acquisite in ambito data center sulle tecnologie Cisco, Vmware e Emc. Le piattaforme VCE nascono dall'integrazione tecnologica dei tre vendor e abbinano virtualizzazione, networking, computing, storage, sicurezza e tecnologie di gestione. Si tratta di soluzioni preconfigurate con l'obiettivo di ridurre la complessità e i rischi di implementazione e quindi di accelerare l'adozione di infrastrutture ottimizzate, convergenti e cloud-based. Magirus distribuirà la tecnologia VCE in tutta Europa e in Medio Oriente in linea con il nuovo Partner Programme VCE. Un elemento chiave di questa nuova distribuzione sarà quello di stimolare e attivare il canale. Le piattaforme Vblock affrontano la fascia medio-alta di mercato data center. VCE e Magirus si impegneranno in azioni di marketing congiunte e programmi di sviluppo del canale. Inoltre Magirus offrirà ai rivenditori un supporto facile e veloce nella gestione degli ordini e gestirà il finanziamento e la fatturazione delle piattaforme Vblock.

www.magirusitalia.it
www.vce.com

A.C.R.