TG Soft alla conferenza VB2011 a Barcellona

Dall'azienda, l'unica italiana accreditata all'evento, un resoconto sui temi trattati in questa occasione.

Come accade da 21 anni, anche nel 2011 si è tenuta la conferenza internazionale VB2011 di Virus Bulletin (www.virusbtn.com), organizzata quest'anno dal 5 al 7 ottobre a Barcellona.
Virus Bulletin dal 1991 organizza conferenze annuali che costituiscono un importante evento per l'industria internazionale anti-malware, durante le quali si incontrano alcuni tra i maggiori ricercatori e specialisti di sicurezza provenienti da tutto il mondo.
TG Soft, che da quasi 20 anni si occupa di tenere al sicuro i pc dei propri utenti, è stata l'unica azienda italiana accreditata alla conferenza, con due delegati, **Gianfranco Tonello**, ingegnere e responsabile dell'area di ricerca e sviluppo e **Roberto Spagliccia**, sviluppatore e ricercatore nel campo anti-malware.

Gianfranco Tonello, responsabile dell'area di ricerca e sviluppo di TG Soft

Malware in evoluzione

Durante l'evento sono stati toccati argomenti riguardanti l'evoluzione dei malware. I tre principali temi di interesse per la generalità degli utenti, hanno riguardato in particolare la diffusione dei fake antivirus (FraudTool), l'evoluzione dei Rootkit come TDL4 e 0Acces o Yoshi, passando per le nuove strategie di social engineering usate per portare attacchi scam su social network a larghissima diffusione come Facebook e Twitter. Attenzione è stata anche dedicata alla diffusione dei nuovi malware su Android e sul loro studio in ambiente chiuso senza il rischio che possano essere diffusi durante la loro analisi su dispositivi mobili.
L'intera industria AV sta seguendo la spinosa questione dei Fake AntiVirus, o FraudTools. Il problema che più preoccupa gli esperti del settore, è la grandissima diffusione di sample diversi, derivati però dallo stesso file di partenza, che fa sembrare tutti questi malware identici, quando in realtà il file portatore è modificato ad arte di ora in ora, per non essere identificato dagli AntiVirus. In questo modo diventa molto difficile riuscire a intercettare tutte le singole varianti. Quello che per un utente può sembrare sempre la stessa versione dello stesso falso antivirus, in realtà usa un file completamente diverso da tutte le versioni precedenti, rendendone impossibile la classificazione secondo la famiglia o la tipologia del file, come sottolineato da diverso tempo da TG Soft (per maggiori dettagli consultare la sezione News sul sito www.tgsoft.it a partire dal mese di Ottobre 2009).
Per far fronte in modo più efficace a queste problematiche, è fondamentale avere un rapporto diretto con il supporto tecnico del prodotto antivirus che si è adottato, proprio come avviene con Vir.IT eXplorer.
Sul versante dei Rootkit, sono state evidenziate le tattiche usate per evitare l'individuazione da parte degli antivirus, agganciandosi ai driver di sistema e/o infettando l'mbr o modificando la memoria per alterare il comportamento del sistema operativo e nascondere altri file. I risultati di questa ricerca sono in linea con i comportamenti già rilevati sul campo dai ricercatori di TG Soft e dalle analisi fatte con tecniche di reverse engineering su vari campioni in possesso del C.R.A.M. (Centro ricerche anti-malware di TG Soft). Si è discusso anche delle contromisure e dei metodi di rimozione utilizzati; Vir.IT eXplorer è uno dei pochi prodotti in grado di rimuovere in modo automatico infezioni da TDL4 e in alcuni casi anche da 0Access (identificato come Yoshi da TG Soft).
Sfruttando la diffusione dei social network come Facebook e Twitter, i virus writer stanno facendo largo uso di queste nuove piattaforme per diffondere le loro 'creazioni'. È sempre più comune che siano usate tecniche di social engineering per portare l'utente a eseguire le azioni volute dal virus writer. Infatti, qualunque link, notizia o

commento potrebbe celare un pericolo nascosto e che incuriosisca il lettore per convincerlo a cliccare, contribuendo alla diffusione dell'agente malware. Infatti, la maggior parte delle pagine pericolose, include al suo interno un Iframe nascosto che però ricopre tutta la superficie della pagina. In questo modo, qualsiasi sia il punto in cui il visitatore clicca, il creatore della pagina ottiene un click sull'Iframe, che simula un click sul pulsante 'Mi Piace' o 'Condividi'. Questo procedimento è definito Click Hijacking, ovvero dirottamento di click, proprio perché il click dell'utente è 'rapito' e dirottato in un posto totalmente diverso da quello di origine. Il risultato è che chi visita la pagina, la ricondivide immediatamente sul suo profilo, senza il bisogno di interazione. Gli amici, incuriositi da titoli accattivanti che spesso riguardano le ultime notizie di gossip, tendono a cliccare a loro volta sulla pagina, contribuendo così alla diffusione, seppure involontaria, della catena. I link proposti da queste pagine portano ovviamente a siti adibiti a diffondere malware, siti adibiti al phishing o che propongono facili guadagni in pochissimo tempo sotto la condizione di pagare una piccola quota di iscrizione, sulla falsa riga del classico multi-level marketing.
Infine, come curiosità sulle tecniche di analisi di malware per dispositivi mobili, è stato presentato un esperimento condotto per studiare il comportamento di questo tipo di malware, usando una rete GSM costruita ad arte, su cui far replicare i sample che, furbescamente, rimarrebbero in attesa del vero segnale, per poi diffondersi quando il dispositivo acceda alla rete. È stato così progettato un piccolo sistema chiuso per simulare un operatore GSM in un laboratorio.
Data la crescente proliferazione di virus/malware di nuova generazione di notevole complessità, il consiglio di TG Soft è quello di usare almeno un antivirus aggiornato con continuità e integrarlo con Vir.IT eXplorer Lite -Free Edition-, appositamente reingegnerizzato per essere compatibile con altri antivirus già presenti nel sistema, senza produrre conflittualità o rallentamenti.
Vir.IT eXplorer Lite è reso disponibile gratuitamente sul sito di TG Soft ed è utilizzabile legalmente sia in ambito privato sia aziendale.

www.tgsoft.it

A.C.R.

La conference phone targata **Konftel**

Konftel 300M, distribuito da Celte, ha caratteristiche innovative rispetto ai modelli resi disponibili in precedenza dall'azienda.

Konftel, leader europeo nel settore audioconferenza, ha ideato una soluzione per le aziende che desiderano dotarsi di un sistema di conference phone, senza intervenire sul proprio impianto telefonico. Il nuovo modello Konftel 300M impiegando una tecnologia GSM e una semplice Sim, coniuga le caratteristiche di un cellulare alla qualità audio unica di Konftel. Ciò che lo rende così innovativo è la nitidezza del suono di cui è dotato, grazie a OmniSound 2.0, l'autonomia di 30 ore, la comodità di ricarica, la tastiera e il display chiari, la possibilità di inviare SMS, le chiamate multiple più agevoli, nonché la possibilità di registrare riunioni su una scheda di memoria.

Ciò che lo rende unico è il fatto di poter essere utilizzato in ambienti dotati di sistemi di comunicazione unificata.
Una volta che la batteria è carica e la carta Sim inserita, Konftel 300M, distribuito da Celte S.r.l. massimizza la produttività, soddisfacendo le esigenze di comunicazione.
Konftel nominato 'Prodotto dell'anno 2008 e 2009' e 'Best of Open Source' nel 2010.

www.celte-srl.com

A.C.R.