

WWW.MATTEOCARLI.COM - I cinesi attaccano le PMI italiane, ne siamo sicuri?

Tra gli articoli di Punto informatico della scorsa settimana me ne è rimasto impresso uno intitolato: I cinesi attaccano le PMI italiane.

Da una indagine compiuta su un campione di 500 PMI italiane del nordest - spiega Mirko Gatto di Yarix - si evidenzia come addirittura il 49% dei casi provenga dalla Cina.

Ma quali categorie di PMI sono incluse nel campione? Cosa è stato fatto sui sistemi, una volta attaccati?

Senza questi dati mi è difficile credere allo spionaggio industriale; magari aziende in settori poco appetibili vengono attaccate quanto aziende molto interessanti per i concorrenti cinesi.

Anche la percentuale di IP cinesi registrati negli attacchi non deve essere sottovalutata. Ma chi assicura che non siano stati usati come testa di ponte?

Tra gli attacchi più utilizzati, segnalati da Yarix, vi sono anche i Cross-site Scripting (XSS). Monitorando l'utilizzo di questi ultimi sul sito vittima, non sarebbe così difficile tracciare il vero intento di un attacco. L'XSS infatti è veicolato dalla "macchina" ma sicuramente il fattore determinante, per una buona riuscita, è quello umano.

In particolare, sul campione di 500 PMI, sono stati registrati 122.500 attacchi nei primi sei mesi del 2007.

Sono abbastanza sicuro che almeno la metà di quegli attacchi era automatizzato o comunque finalizzato alla compromissione della macchina per utilizzi come "Malicious Web Server" o semplice defacement.

Speravo in un report dettagliato, ed invece nemmeno sul sito Yarix, azienda fonte della notizia, si trova niente. Peccato perchè la cosa è molto interessante.

Update: noto con piacere che non sono l'unico a pensarla in questo modo: Attacchi dalla Cina alle PMI?, di Claudio Telmon.

<http://www.telmon.org/?p=204>

« Online banking security barcamp a Viareggio
Owasp Day a Roma »

Attacchi dalla Cina alle PMI?

Così direbbe Yarix secondo quanto riportato da Punto Informatico. Peraltro, io sul sito di Yarix non ho trovato traccia di questa notizia, che mi interessava approfondire. Certo che, così com'è data su Punto Informatico, la notizia non sembra avere una base molto solida. Prima di tutto, la statistica comprende phishing, spam, virus e tutto il solito bestiario. Di questo, il 49% verrebbe dalla Cina (ovvero da IP cinesi). In effetti, la statistica che citano ha una distribuzione che mi giunge nuova, più per il 25% della Turchia che per il 49% della Cina. Poi vengono elencate le tecniche di attacco: Cross Site Scripting ecc...

In realtà, nessuno dei dati presentati si può mettere direttamente in relazione con lo spionaggio industriale. Partendo da quei dati, la notizia poteva essere titolata in molti altri modi, anche più legati ai dati raccolti (ad esempio: "Le PMI sono appetibili come zombie?").

Il problema è che l'indagine è concentrata sulle tipologie di attacco (e sul paese di provenienza), non sugli obiettivi o gli effetti dell'attacco. Ad esempio, gli attaccanti potevano appunto essere alla ricerca di zombie. Ci sono altre informazioni che suggeriscono lo

spionaggio industriale? Per quello mi interessava il report originale. Ad esempio, se ci fossero indicazioni che determinate categorie di PMI sono più attaccate di altre, allora sarebbe più facile dedurre qualcosa sullo spionaggio industriale; se invece le PMI che producono oggetti appetibili hanno la stessa percentuale di attacchi di tutte le altre, allora è difficile parlare di spionaggio industriale. Oppure, servirebbero informazioni su cosa è stato fatto sui sistemi attaccati.

Insomma, come dice Punto Informatico, "Lo spettro dello spionaggio industriale telematico si è già affacciato in passato". Si è già affacciato perché è decisamente credibile: se è vero che i cinesi sono interessati ad avere in anticipo i modelli italiani, lo spionaggio telematico è uno strumento per ottenerli con poco sforzo, poco rischio e senza muoversi da casa. Tuttavia, sembra essere ancora uno spettro, appunto.

FONTE: <http://www.matteocarli.com/2007/09/i-cinesi-attaccano-le-pmi-italiane-ne-siamo-sicuri.html>