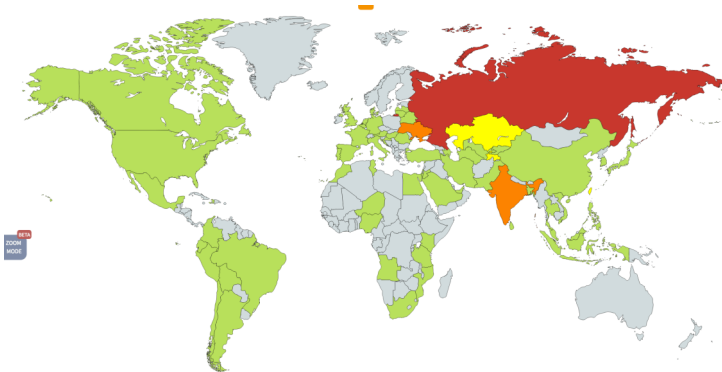


Il Ransomware WannaCry sta tenendo col fiato sospeso mezzo mondo. Migliaia di computer nel giro di un weekend sono stati infettati compromettendo i dati di istituzioni, aziende e servizi pubblici.

Cosa rende diverso WannaCry da altri noti Ransomware? Semplice: per propagare questo virus non serve un errore umano (ad esempio l'apertura di un link su una e-mail infetta) ma viene sfruttata una falla individuata nei sistemi Windows.

In realtà Microsoft già a marzo aveva scoperto questo grave problema e rilasciato un aggiornamento che metteva in sicurezza i sistemi.



Ma allora, perché questo attacco è stato così devastante?

Ancora una volta la risposta è semplice: gran parte dei computer di istituzioni e aziende non è aggiornato all'ultima release del sistema ed i vecchi Sistemi Operativi come Windows XP o Vista sono ancora molto diffusi.

Microsoft ha rilasciato una patch di emergenza anche per questi sistemi ma ormai il danno è fatto e purtroppo, ad oggi, non esistono sistemi in grado di decriptare i dati coinvolti in questo attacco cyber criminale. Non è nemmeno sicuro che il pagamento del "riscatto" in Bitcoin richiesto possa rilasciare la giusta chiave per ripristinare i propri dati.

Come proteggerci?

Quando si parla di obsolescenza informatica non si parla solo di Hardware che invecchia e di macchine che diventano lente. I veri problemi sono dati proprio dalla mancanza di aggiornamenti dei sistemi che così diventano troppo vulnerabili ed attaccabili. Buona parte della vita degli individui ormai è indiscutibilmente digitale: operazioni bancarie, fotografie di famiglia, Social Network, documenti personali. **Proteggiamo la nostra vita digitale aggiornando sempre i sistemi (in alcuni casi è proprio necessario sostituire i computer), utilizzando un buon antivirus e soprattutto effettuando sempre back-up su dispositivi esterni.**



DIGITAL NETWORK S.R.L.
Consulenze Informatiche & Networking