Un’epidemia di ransomware ha colpito l’Italia

- Artuto Di Corinto, 12.08.2021

Hacker's Dictionary. È ora di alzare le difese

Ce lo aspettavamo ed è successo: l’Italia è il terreno di una nuova pandemia, informatica stavolta. E a niente sono servite le precedenti avvisaglie quando due attacchi cibernetici, che hanno coinvolto i fornitori di tecnologie SolarWinds e Kaseya, hanno portato scompiglio nel nostro paese.

É di ieri la notizia che anche Accenture è sotto scacco delle gang del ransomware Lockbit 2.0, un software malevolo in grado di installarsi nei sistemi della vittima impedendogli di accedere a file e risorse fino al pagamento di un riscatto.

Bersaglio di Lockbit 2.0 sono state parecchie realtà produttive e industriali del nostro paese in queste settimane: Erg, che produce e trasporta energia, Acquazzurra Firenze, e all’estero la città di Nottingham (Uk), BioAgri, Ymca e Swift Logistics (Usa).

Mentre vittime di Ransomeex, l’altro ransomware venuto alla ribalta con la paralisi della Regione Lazio, sono state il Consiglio nazionale del notariato, Ermenegildo Zegna Holding, eccetera. La lista è lunga e la potete trovare su doubleextortion.com, un sito creato dall’ingegnere italiano Luca Mella che tiene traccia di tutti i tentativi di estorsione che i gruppi criminali pubblicano sui loro siti nel dark web, la parte del web accessibile solo con software specifici come Tor (The Onion Router) dove si incontrano però anche dissidenti politici e religiosi, investigatori e giornalisti in cerca di anonimato e non solo criminali.

Secondo alcuni ricercatori, gli affiliati di Lockbit avrebbero addirittura passato credenziali rubate e strumenti da scasso ad altri criminali, come forse a quelli della gang Ransomeex, e i membri della due gang adesso collaborerebbero tra di loro.

La maggior parte delle volte questi software malevoli (virus o worm) penetrano le difese di aziende ed organizzazioni a causa delle cattive pratiche degli utenti, come quelle che ci invogliano ad evitare ToothPic, Panda Security, Ermes security con i loro consigli: non usare lo stesso dispositivo per lavoro e divertimento, non prestarlo ai figli, non lasciarlo incustodito, mai collegarsi a una rete pubblica insicura, usare password robuste su pc, tablet e telefoni.

Questo dal lato utente.

Ma c’è un problema sistemico. Come ha correttamente osservato il professore di cybersecurity Aaron Visaggio, “bisogna focalizzare due questioni: a) la potenza di fuoco del cyber crime sta crescendo in modo esponenziale in capacità, infrastrutture, software utilizzati; b) molti ransomware sono chiaramente evasivi rispetto ai controlli. Al di là delle promesse di eccellenza degli strumenti che usiamo, è fin troppo chiaro che utilizziamo paradigmi fallimentari nell’individuazione delle minacce”.

Rincara la dose Mariana Pereira di Darktrace secondo cui le minacce ormai provengono da ogni direzione, sfruttano le tattiche di social engineering e altri strumenti avanzati, e gli attacchi avvengono in pochi millisecondi, più velocemente di quanto qualsiasi team di sicurezza possa reagire. Inoltre, molti attacchi informatici riescono a eludere i controlli e iniziano a diffondersi in modo aggressivo negli ambienti aziendali. “Per questo credo che la resilienza delle organizzazioni oggi non possa più dipendere dal numero limitato di persone che operano nel team di security, o

dallaggiornamento sulle competenze, perché il ransomware non è più un problema affrontabile e risolvibile con la sola capacità umana: gli attacchi sono sempre di più e sfruttano l'Intelligenza Artificiale, e abbiamo bisogno di una risposta capace di adattarsi alla loro stessa velocità di propagazione".

È ora di alzare le difese.