volerelaluna LA POLITICA PUNTOACAPO

La vera minaccia dei software spia non è quello che ascoltano

Autore: Umberto Rapetto

Poche righe di codice informatico possono essere più pericolose di un chilo di tritolo. Non è questione di consistenza, peso o dimensione dell'arma letale: se si vuol "uccidere" qualcuno non c'è alcun bisogno di strumenti di tradizionale cruenza. **Può bastare un silenziosissimo e impercettibile software a demolire l'esistenza di un "nemico"**. È il delitto perfetto, privo di qualunque "residuo" che possa costituire traccia. Parliamo di RAT, *Remote access tools*, ovvero dei **programmi che permettono di acquisire il controllo di un dispositivo informatico operando da remoto, ossia senza aver alcun bisogno di avere fisicamente tra le mani l'oggetto da "rimaneggiare" e poi gestire**.

Questo genere di invisibile "telecomando" è quello che trasforma chi se ne serve nel regista incontrastato e incontrastabile del destino dell'apparato e, soprattutto, di quello del legittimo possessore di tale aggeggio hi-tech. Lo smartphone (o il tablet o il personal computer) improvvisamente inizia a condurre una seconda vita, parallela e inavvertibile da chi lo porta al seguito. **Tutti sono portati a pensare al rischio di essere ascoltati, pedinati, depredati di ogni segreto**. Non sanno che quelle preoccupazioni sono ben poca cosa rispetto i reali danni che un RAT (o Trojan come a molti piace identificarlo) è ragionevolmente in condizioni di causare al soggetto nei confronti del quale viene irriguardosamente brandito.

Se il software in questione è pilotato da soggetto privo di qualsivoglia scrupolo, il programma non si limiterà ad usare il microfono per acquisire le voci, la videocamera per fotografare o filmare quel che è a tiro di ripresa, i testi delle chat e delle mail per avere copia di ogni tipo di corrispondenza, l'audio delle telefonate normali e di quelle eseguite o ricevute con WhatsApp o altri sistemi analoghi, il materiale pubblicato sui social, la navigazione web, il contenuto dell'agenda e della rubrica fino a quel momento custodite gelosamente, il traffico telefonico in ingresso e in uscita, la ricostruibile rete di contatti di più varia natura… È un elenco lungo, terribile e doloroso.

A mettere in angosciante allarme non è quel che può essere saccheggiato e trasmesso – nottetempo o quando il telefono rimane inerte per un certo arco temporale – al server che colleziona quanto quotidianamente viene fagocitato dal RAT. Lo spavento traumatico non riguarda il bottino che l'utilizzatore di Graphite, Pegasus o altre diavolerie è in grado di asportare dall'arnese nel mirino, ma quel che è in grado di "caricare" al suo interno all'insaputa del legittimo detentore e utilizzatore.

L'accesso da remoto equivale in termini pratici ad essere seduti alla tastiera del computer controllato o ad avere tra le mani il "telefonino intelligente". **Chi ha in mano la cloche virtuale di quell'attrezzo può raccogliere e memorizzare a bordo il materiale più**

orribile e compromettente che si possa immaginare, facendo risultare che inserimento e conservazione di certa robaccia siano da addebitare al proprietario dello smartphone o del laptop.

Il dispositivo spiacevolmente spiato può tramutarsi nel contenitore di nefandezze o di immateriali corpi di reato. La persona da origliare e sorvegliare diventa improvvisamente un criminale: **foto pedopornografiche o appunti a connotazione terroristica, naturalmente nascosti perché il soggetto non se ne accorga e non ne immagini la presenza, diventano la "prova" di quel che non si è nemmeno mai immaginato di commettere**. Lo si vada a raccontare alla gente di essere estranei a simili storie. Si è morti, senza aver sentito neppure il sibilo del proiettile.

L'articolo è tratto da *il manifesto* dell'8 febbraio