Informatica e democrazia: nulla di scontato

Leggo oggi, con grande interesse, l'intervista che viene pubblicata sul blog del collettivo Autistici/Inventati a Claudio 'Nex' Guarnieri, ricercatore del progetto citizenlab.org ed esperto di sicurezza informatica.

Come si legge all'inizio dell'articolo:

> *secondo noi e' interessante per due motivi:*
>
> *1) Delinea una visione critica del mondo della sicurezza informatica visto dall'interno.*
>
> *2) Citizenlab fa un gran lavoro sui malware come strumento di controllo, spesso rivolto nei confronti di attivisti politici.*
> *In Italia si sta tentando di inserirli nella legislazione come "Captatori Informatici" (un termine che rimanda agli "Elaboratori Computazionali" e ai tecnici in camice bianco…), perché malware, backdoor, trojan suonavano evidentemente male.*

E già qui si entra in un ambito interessante: nell'intervista viene raccontato come l'industria della "sicurezza" informatica campi sull'**insicurezza** informatica, e come l'alimenti; e già questo basterebbe a rendere interessantissimo l'articolo. Ma, di più, si racconta come

siano gli stessi stati – spesso quelli definiti “paladini della democrazia” – ad usare questi metodi, per tutelare la “democrazia”. Uccidendola.

In tutto questo malsano gioco mi ha colpito molto un passaggio. Da Linux user quale sono ho sempre pensato non di essere esente da questi attacchi – tipici del mondo Windows – ma almeno un po’ più tutelato alla base. Non è così, e Guarnieri ce lo spiega benissimo:

> ***C – Ma supponiamo che un utente utilizzi Linux, aggiorni il suo sistema quotidianamente, si doti di full disk encryption, gestisca con attenzione la sicurezza fisica della sua macchina e navighi facendo uso di VPN affidabili e sistemi di anonimato forte. Neanche in quel caso può ritenersi al sicuro?***
>
> *N – No. Se il tuo avversario è motivato e dispone di sufficienti risorse può arrivare a livelli di sofisticazione elevati. Backdoor, exploit e 0day per Linux non mancano: ci sono società che producono esclusivamente quelli. I loro prodotti, venduti regolarmente a governi di tutto il mondo, costano di più. Ne consegue quindi che per attaccare target dotati di maggiori competenze tecniche è necessario un maggior investimento economico. Maggiori layer di sicurezza frapponi tra te e loro, maggiormente sarai in grado di farli desistere dalle loro intenzioni.*
>
> *Va considerato però che che sarebbe stupido provare a colpire un utente più tech savvy: è molto più probabile e sensato che un attaccante diriga la sua attenzione su persone sprovviste delle competenze necessarie per difendersi e tramite esse provi ad ottenere informazioni relative a tutto il suo network di appartenenza. Anche questa è una tattica molto comune che abbiamo visto verificarsi più volte in passato.*

Cosa significa questo passaggio? Due cose fondamentali:

1. che anche noi Linux user, magari pure avanzati (o che ci crediamo tali) NON siamo al sicuro, anche se usiamo tutte le strategie possibili ed immaginabili; e che bisogna continuare a trovare soluzioni che tutelino la nostra privacy e quella degli altri;
2. che anche se riuscissimo nell'arduo compito detto sopra, comunque non basterebbe, perché se anche UN solo anello della nostra catena di relazioni è debole, tutta la catena cade.

Questo significa che DOBBIAMO continuare a fornire strumenti, conoscenza e – SOPRATTUTTO – **consapevolezza** su cosa sia, oggi, il mondo dell'informatica (e quindi personal computer, portatili, smarphone, console e via discorrendo) e quanto sia importante che TUTTI ci regoliamo di conseguenza.