«Spyware di Stato, sempre più invasivi ed efficaci»

- Chiara Cruciati, 28.03.2021

Medio Oriente social. Intervista all'esperto di sicurezza informatica Claudio Guarnieri: «La sorveglianza di attivisti e giornalisti accompagna persecuzione giudiziaria, campagne di diffamazione, disinformazione orchestrata tramite reti di troll e bot su social media»

Claudio Guarnieri, esperto di sicurezza informatica a capo del Security Lab di Amnesty, nelle sue ricerche ha trattato dettagliatamente l'uso di spyware in Medio Oriente nel controllo sociale e il tracciamento dati. Quanto è cambiata la situazione negli ultimi 10 anni nell'uso e la diffusione di questi strumenti?

L'utilizzo di spyware e di altre forme di attacco informatico è in continuo aumento, in Medio Oriente come in ogni altra parte del mondo. La crescente ubiquità della crittografia nelle comunicazioni, si pensi a WhatsApp come a Signal, è stato forse il fattore più importante. Nonostante sia positivo che le nostre comunicazioni siano più sicure che mai, ha anche inevitabilmente influenzato la crescente popolarità di strumenti più invasivi, come spyware, per poter «rimediare» all'inadeguatezza delle intercettazioni più tradizionali. Casi di telefoni e computer «infettati» con spyware di Stato ormai sono quasi all'ordine del giorno, in particolar modo contro giornaliste/i e attiviste/i di diritti umani che lavorano in zone a rischio.

Tra le pratiche adottate c'è il cosiddetto phishing che ha permesso negli ultimi anni di prendere di mira centinaia, migliaia di attivisti, giornalisti, oppositori. Come funziona, quanto è diffuso e quanto è efficace?

Phishing è una forma di attacco molto comune, che ha lo scopo di ottenere accesso illegitimo ad account online, come email e social media, della vittima. Tipicamente l'attaccante cerca di ingannare la vittima ad autenticarsi in una pagina login verosimile al servizio originale e ottenere così la password di accesso. Può sembrare banale, ma nel nostro lavoro osserviamo spesso attaccanti più risoluti che spendono anche mesi a creare false identità, infiltrare comunità online, creare legami via social media, prima di eventualmente azionare l'attacco senza creare il minimo sospetto. È in assoluto la tattica più diffusa, più «economica» e nonostante ciò abbastanza efficace e per questo spesso utilizzata su larga scala.


Claudio Guarnieri

In questi anni un prodotto molto ambito è stato l'israeliano Pegasus della Nso, utilizzato da diversi governi della regione, come abbiamo visto in Marocco e il caso di controllo di giornalisti locali. Quanto è diffusa la «messa in comune» di tali strumentie quali sono le società regionali ed europee più presenti in Medio Oriente con i loro prodotti?

L'utilizzo di spyware come Pegasus è ormai quasi la prassi. Sono strumenti sofisticati e costosi, ma comunque sia a buon mercato per governi, forze di polizia, militari e intelligence di tutto il mondo. In Medio Oriente, specialmente in Nord Africa e nel Golfo Persico, il loro utilizzo èquasi tradizione e molti casi di giornaliste/i, attiviste/i e dissidenti spiati con questi spyware sono venuti alla luce già dal 2011 durante il movimenti di protesta nella regione e continuano oggi. Al tempo l'italiana Hacking Team e la tedesca FinFisher erano i produttori più conosciuti, oggi Nso forse mantiene il podio, ma è un'industria che esiste nell'ombra in cui operano dozzine e dozzine di società.

La sorveglianza online è considerabile una violazione del diritto internazionale?

L'utilizzo illegittimo della sorveglianza online può essere una violazione dei diritti umani alla privacy e alla libertà di espressione. Se non vengono utilizzate all'interno di un framework legislativo restrittivo, con appropriati controlli e autorizzazioni e se diventano invece strumenti di controllo del dissenso, i rischi di abuso sono molto alti.

È possibile capire quanto la sorveglianza online sia ormai integrata nei sistemi governativi di controllo sociale, accanto alle pratiche più «antiche» e se il suo utilizzo ha condotto a effetti concreti (chiusura di giornali o di ong, arresti e condanne?

È importante capire che la sorveglianza online non è un fenomeno a sé, ma fa spesso parte di meccanismi di repressione più complessi. Voglio ricordare attivisti e giornalisti come Ahmed Mansoor negli Emirati, Omar Radi e Maati Monjib in Marocco, tutti vittime di spyware e a oggi imprigionati per il loro dissenso. La loro sorveglianza ha accompagnato persecuzione giudiziaria, campagne di diffamazione su stampa di Stato, così come disinformazione orchestrata tramite reti di troll e bot su social media. Negli anni ne abbiamo viste di ogni: dall'utilizzo di tracciamento Gps per individuare la posizione di attivisti da molestare e assalire, all'utilizzo di spyware per filmare tramite la webcam momenti intimi di giornaliste e giornalisti usati come ricatto per far chiudere i loro giornali. Pretendere che queste tecnologie siano solo innocui strumenti investigativi è solo un modo per infilare la testa nella sabbia.