La polizia indiana usa gli hacker per arrestare gli attivisti

Il gruppo di ricercatori statunitensi di **SentinelOne** è incappato in prove capaci di dimostrare che la polizia di Pune, quarta città industriale dell'India, **sia direttamente collegata all'hacking dei profili digitali degli attivisti** Rona Wilson e Varavara Rao, nonché del professore Hany Babu dell'Università di Delhi University, soggetti che sono stati arrestati tra il 2018 e il 2020 con l'accusa di terrorismo.

I tre accusati fanno parte di un gruppo di sedici arresti, i cosiddetti "Bhima Koregaon 16". Si tratta di sedicenti estremisti di sinistra che sono stati imprigionati per aver fomentato sommosse violente che hanno portato ad almeno due morti, tuttavia le prove che dimostrerebbero la loro colpevolezza sono state contestate in molteplici occasioni e tutto da a intendere che queste siano state **profondamente falsificate**.

SentinelOne, ma anche la nonprofit Citizen Lab e Amnesty International hanno fornito negli anni diverse prove del fatto che le detenzioni si appoggino ingiustamente su elementi ricavati attraverso attacchi di phishing, via spyware e utilizzando i software per cui è ormai divenuta celebre l'azienda israeliana NSO Group, Pegasus in primis. La novità non è dunque che attivisti, accademici e giornalisti siano stati colpiti massivamente con questi stratagemmi, quanto il fatto che **le manovre incriminate siano ora direttamente collegabili alle autorità locali**.

Il come si sia giunti a questa conclusione è allo stesso tempo semplice e disarmante: grazie al **sostegno di un'email provider** che ha preferito mantenere l'anonimato, i ricercatori si sono resi conto che le caselle di posta di Wilson, Rao e Babu hanno registrato come contatto di backup il medesimo numero di telefono. Il collegare il proprio profilo a un numero di cellulare è sempre utile per accedere alla propria e-mail qualora ci si dimentichino i dati di accesso o nel caso si verifichi un furto d'identità, tuttavia il fatto che i tre avessero optato per un unico riferimento è quantomeno sospetto, soprattutto considerando che il telefono in questione, sostiene lo staff di SentinelOne, è registrato a nome di un ufficiale di polizia coinvolto proprio nel caso dei Bhima Koregaon 16.

«Esiste una connessione dimostrabile tra gli individui che li hanno arrestati e gli individui che hanno piazzato le prove», ha dichiarato Juan Andres Guerrero-Saade, ricercatore dell'azienda statunitense, alla testata *Wired*. Guerrero-Saade e i suoi colleghi hanno scoperto in passato che la campagna di hacking – battezzata internamente come "Elefante Modificato" – sia stata avviata originariamente nel 2012 e che quindi sia andata a intensificarsi strada facendo, raggiungendo il massimo picco di aggressività nel 2014 per proseguire almeno fino al 2016.

Risulta interessante notare che queste ultime, importanti, rivelazioni non giungano tanto in

risposta a investigazioni giornalistiche, né sono la diretta conseguenza di un'analisi informatica particolarmente profonda. La situazione si è sbloccata più che altro per una scelta etica del già menzionato e-mail provider, il quale ha deciso di prendere una posizione netta, per quanto potenzialmente illegale. «Di solito non riveliamo alle persone da chi sono state attaccate», ha riferito un analista dell'azienda coinvolta, «ma sono stufo di stare a guardare. Questi tizi non stanno dando la caccia ai terroristi. Stanno dando la caccia ai difensori dei diritti umani e ai giornalisti. E non è giusto».

[di Walter Ferri]