Domenica 12 dicembre, sono comparsi sugli anfratti loschi della Rete alcuni file sensibili che riguardano l'Italia. Un utente noto solamente con il *nom de guerre* zerox296 ha infatti pubblicato sui forum Raidforum e Xss dei documenti riguardanti la **Sogin**, documenti che riguardano perlopiù dei carteggi relativi al progetto Cemex dell'Eurex di Saluggia. Si trattava di un piano che mirava a creare dalle parti di Vercelli un vascone di cemento da 230 metri cubi in cui depositare scorie radioattive liquide, piano che è stato poi rivisto a causa della lentezza dei lavori.

Non una lettura particolarmente accattivante agli occhi delle masse, ma ciò che è stato esibito può comunque risultare utile nella macrosfera dello spionaggio industriale/governativo, inoltre non è che un assaggio di quello che hanno in mano i cybercriminali. **I documenti non erano che un piccolo esempio** con cui dimostrare che i contenuti trafugati sono "legittimi" e affidabili, così da invogliare i papabili acquirenti a farsi avanti con una proposta d'acquisto. Quello che si può consultare in chiaro non è dunque che la punta dell'iceberg, un iceberg la cui portata è stimata sui **800 GB** e per cui gli hacker chiedono circa 250mila dollari sotto forma di criptovalute.

Sogin, vale la pena ricordare, è l'azienda statale che si occupa di *decommissioning* – ovvero di smantellare gli impianti nucleari – e di **gestione dei rifiuti radioattivi**, una realtà che opera innegabilmente in un contesto sensibile, soprattutto ora che il discorso nazionale è tornato a propagandare l'importanza "green" ed economica della rivalutazione delle opzioni energetiche di origine nucleare, le quali sembravano ormai state accantonate dal referendum del 2011. La società con partecipazione diretta del Ministero dell'Economia e delle Finanze ha altresì commentato la situazione con una lapidaria nota stampa in cui si limita a riconoscere l'esistenza dell'attacco hacker e a segnalare che l'operatività e la sicurezza degli impianti sia garantita.

Lo scarno comunicato non offre nessuna lettura sugli elementi più importanti della faccenda, ovvero **come questa fuga di dati sia avvenuta e quale sia la portata del danno**. Sappiamo grosso modo che i criminali hanno messo le mani su dati sensibili quali contratti, curriculum vitae dei collaboratori, cartografie e certificazioni di sicurezza, ma non è dato sapere se le informazioni siano state raccolte con un vero e proprio attacco, attraverso il cosiddetto *data scraping*, se siano state intercettate in un Cloud o, per assurdo, se qualche malintenzionato sia incappato in una memoria esterna custodita troppo goffamente.

Si tratta di un *omissis* gigantesco, visto che l'Italia, omologandosi all'Occidente intero, si sta tuffando a capofitto nella digitalizzazione, cosa che a sua volta si tradurrà nel tempo in una lievitazione esponenziale delle fughe di dati e degli attacchi informatici. Non solo risulta

dunque necessario consolidare in maniera quasi ossessiva la sicurezza informatica delle infrastrutture sensibili, ma si rende indispensabile già da adesso la **definizione di un protocollo comunicativo che garantisca al pubblico massima trasparenza** sull'effettiva portata dei danni.

Negli 800 GB persi da Sogin ci sono molti contenuti irrilevanti, ma anche password e chiavi d'accesso di cui è difficile intuire la destinazione d'uso. Una simile ignoranza sarebbe già discutibile se stessimo parlando di un qualche servizio di intrattenimento quale potrebbe essere il video-streaming, tuttavia qui stiamo prendendo in analisi un'azienda che tratta materiali dannosi e che collabora gomito a gomito con realtà quali Enel e Leonardo, anche se venisse fuori che le informazioni trafugate sono innocue, questo episodio può essere interpretato come un pragmatico segnale d'allarme che dovrebbe spingere le autorità a intensificare grandemente gli sforzi preventivi e gestionali di una nazione che vuole informatizzare ogni suo minimo aspetto.

[di Walter Ferri]