Il sequestro Lockbit, operazione Cronos

di Edoardo Limone

Il 20 febbraio 2024, alle ore 11:00 GMT, **oltre dieci forze di polizia** hanno comunicato di aver interrotto gli affari illeciti del **Team LockBit**, autore di molteplici *data breach* in tutto il mondo. L'**operazione Cronos** è stata come un tuono: improvviso e fragoroso e ha prodotto stupore e incredulità ma non in tutti. In molti, infatti, si sono accorti che tra tutte quelle "*bandierine*" posizionate sul comunicato, mancava quella italiana; tra tutti i loghi delle forze di polizia coinvolte, mancava quella dell'*ACN* o della *Polizia Postale*, insomma l'Italia era una grande assente.

Eppure, tra le vittime italiane c'erano aziende molto note, ricordiamo la **Rovagnati**, l'**Ente Nazionale del Turismo**, il **Comune di Gonzaga**; sono novantasei le vittime italiane di LockBit negli ultimi anni e anche se possono sembrare poche, bisogna considerare che l'Italia non può essere paragonata ai numeri degli Stati Uniti d'America. Novantasei target sono molti, sia per numero che per importanza: ricordate lo scalpore del data breach all'**AULSS 6 Euganea** di fine 2021?

L'Italia che fine ha fatto? Che ruolo ha nel contrasto a queste *cybergang*?
Cronos ha visto la partecipazione di:

- **Francia**: Gendarmeria Nazionale (*Gendarmerie Nationale – Unité nationale cyber C3N*)
- **Germania**: Ufficio statale di investigazione criminale Schleswig-Holstein (*LKA Schleswig-Holstein*), Ufficio federale di polizia criminale (*Bundeskriminalamt*)
- **Paesi Bassi**: Polizia Nazionale (*Team Cybercrime Zeeland-West-Brabant, Team Cybercrime Oost-Brabant, Team High Tech Crime*) e Procura della Repubblica Zeeland-West-Brabant
- **Svezia**: autorità di polizia svedese
- **Australia**: Polizia federale australiana (*AFP*)
- **Canada**: Royal Canadian Mounted Police (*RCMP*)
- **Giappone**: Agenzia Nazionale di Polizia (警察庁)
- **Regno Unito**: National Crime Agency (*NCA*), South West Regional Organized Crime Unit (*South West ROCU*)
- **Stati Uniti**: Dipartimento di Giustizia degli Stati Uniti (*DOJ*), Federal Bureau of Investigation (*FBI*) Newark
- **Svizzera**: Ufficio federale di polizia (*fedpol*), Procura del Cantone di Zurigo, Polizia cantonale di Zurigo

RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT

Ha partecipato la **Svizzera**, attaccata 22 volte, ha partecipato la **Svezia**, con 5 target colpiti, ma **non l'Italia** con i suoi 96 target1. Nel comunicato ufficiale dell'Europol2 si legge, tra l'altro, che il successo dell'azione è stato reso possibile grazie al sostegno dei seguenti paesi:

1. **Finlandia**: Polizia nazionale (*Poliisi*)
2. **Polonia**: Ufficio centrale per la criminalità informatica di Cracovia
3. **Nuova Zelanda**: Polizia neozelandese
4. **Ucraina**: ufficio del procuratore generale dell'Ucraina, dipartimento per la sicurezza informatica del servizio di sicurezza dell'Ucraina, polizia nazionale dell'Ucraina

Dell'Italia nemmeno l'ombra, così come è stato silente molto dell'apparato di stampa che si è "svegliato" con **oltre 24 ore di ritardo** rispetto alla notizia.
Ma cosa significa tutto questo? Come possiamo interpretare questa assenza e questo silenzio? In questi anni, contrariamente all'aspettativa di molti l'Italia non ha acquisito una cultura adeguata dei fenomeni globali di cyber terrorismo; esistono senza dubbio aziende che si distinguono per la capacità di ottenere risultati e applicare procedure ma sono una minima parte ma molto dell'apparato di stato, della pubblica amministrazione, è spesso **sofferente di uno stato di disorientamento**.

Lo dimostrano indubbiamente il **mancato rispetto dei livelli di servizio** a danno dei cittadini, che svelano un'impreparazione tecnica e organizzativa nel contrasto all'incidente. Lo dimostra l'incapacità di comunicare correttamente il data breach, sia nell'immediato che nei giorni seguenti alla violazione di sicurezza: la comunicazione è spesso carente di dettagli, tende a minimizzare e, talvolta, non è realmente trasparente.

Anche le aziende private non sono esenti da questi problemi: molte hanno un atteggiamento di negligenza nei confronti delle più comuni **regole di cyber security** al punto che, durante l'analisi dei data leak, si rimane perplessi circa il reale grado di formazione dei dipendenti. **Password** scritte in chiaro in file txt, dati particolari contenuti in formati documentali deprecati, **sconsigliati da AgID**, esposti senza alcuna protezione nelle directory dei server, gestionali accessibili con credenziali a dir poco risibili. Onestamente, se non fosse negligenza, sembrerebbe quasi sarcasmo.

1 **Fonte**: *https://www.ransomfeed.it*
2 **Fonte**: *https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation*

RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT

Giova ricordare che il **Regolamento UE 2016/679** (GDPR) impone che i trattamenti dei dati personali avvengano esclusivamente se l'organizzazione ha le capacità per eseguirli: capacità tecniche e organizzative, conoscenza e adeguata consapevolezza (*accountability*) per poterli trattare. Credo che si debba fare un'attenta riflessione su quanto accaduto in questi anni e sulla posizione che l'Italia ha scelto di avere (o di non avere) nel panorama internazionale della cybersecurity: nel caso qualcuno non se ne fosse accordo **questo non è il futuro ma il presente**.

segui **Edoardo** su

RANSOMFEED | RANSOMFEED.IT | AN ITALIAN PROJECT