

ASL L'AQUILA: TUTTI I DATI SENSIBILI PUBBLICATI ON LINE, ROMANO, "NESSUNA TRATTATIVA CON HACKER"

15 Maggio 2023



L'AQUILA - Con 13 file .rar suddivisi per reparti ospedalieri, il gruppo hacker Monti ha aggiornato la pubblicazione dei dati di operatori sanitari e pazienti (cartelle cliniche, diagnosi oncologiche, aborti, malattie croniche e fisioterapie), così come informazioni organizzative.

Una mole di 386 gigabyte che completerebbe il pacchetto di oltre 522 giga di dati trafugati dalla Asl dell'Aquila la notte del 3 maggio.

La nuova pubblicazione, disponibile nello spazio anonimo del deep web aperta dagli hacker per la gestione dei dati relativi a questo crimine informatico, è accompagnata da un messaggio in cui viene sottolineato che "non è stata avanzata alcuna richiesta di riscatto, i media si sono inventati l'importo".

Una condizione quest'ultima in parziale contraddizione con messaggi precedenti, in cui si chiedeva invece ai vertici di Regione Abruzzo e Asl di arrivare a un accordo.

Lo stesso presidente della Regione Marco Marsilio, ha fatto più volte riferimento a un riscatto, sottolineando la volontà di non voler pagare alcuna somma.

Intanto, sono arrivate le prime azioni legali dei cittadini all'Azienda sanitaria in merito ai gravi disagi provocati all'attività ospedaliera, così come in relazione alla gestione dei dati sensibili.

Si segnalano mail di estorsori sciacalli che chiedono 600 euro per non divulgare i dati sensibili dei pazienti.

Disagi al cup, con persone in fila dopo aver preso i biglietti, sperando di poter effettuare le prenotazioni, "una volta allo sportello però hanno dovuto constatare che gli operatori avevano la possibilità di ricevere solo i pagamenti senza poter effettuare nessuna nuova prenotazione", spiega una paziente.

ASL L'AQUILA: "NESSUN CONTATTO CON GRUPPO MONTI, NESSUNA TRATTATIVA"

"Nonostante la provenienza degli attacchi sia nota, l'Azienda tiene a sottolineare come non vi sia stato contatto alcuno né con il gruppo di hacker, né con chiunque abbia rivendicato la penetrazione nei sistemi di gestione sanitaria. A tal proposito,

risulta quantomai bizzarro che, in assenza di un qualsivoglia canale di comunicazione instaurato con gli hacker, la Asl 1 possa aver appreso l'importo di un presunto riscatto richiesto dai trafugatori".

Così in una nota il direttore generale della Asl provinciale dell'Aquila, Ferdinando Romano, sull'attacco hacker che dal 3 maggio scorso ha messo fuori uso il sistema informatico dell'Azienda sanitaria paralizzando servizi e prestazioni.

Romano parla per la prima volta dopo l'attacco per fare il punto della situazione.

"Proseguono incessanti – spiega – i lavori di ripristino dei sistemi informatici da parte della Asl 1, coordinati dalla task force individuata nei giorni scorsi per attuare la controffensiva ai cyber-attacchi patiti dall'azienda sanitaria e rivendicati dal Gruppo Monti. I CUP dei presidi ospedalieri saranno tutti attivi a partire da oggi e nei prossimi giorni saranno ripristinati i CUP distrettuali".

Nella nota si informa che la Radioterapia "ha iniziato a lavorare a pieno regime sin da ieri, domenica, con sei pazienti. Funzionano inoltre a pieno ritmo sale operatorie e diagnostica per immagini e nei prossimi giorni sarà ripristinata la piena operatività dei laboratori analisi".

"Ricordiamo ai cittadini – conclude poi il direttore generale – che la divulgazione dei dati trafugati costituisce un reato e chiunque scarichi dal dark web file rubati commette un illecito, quindi ribadiamo l'invito a non aprire documenti rilasciati illegalmente in rete".

Ma Romano si sofferma soprattutto sulla decisione di non aver contatti con i pirati che, oltre a Marsilio, hanno chiesto il riscatto anche a lui. "La Asl 1 ha scelto sin da subito di non instaurare alcun tipo di contatto o trattativa con i criminali, bensì di avviare, nel riserbo più assoluto, le attività di indagine, bonifica e ripristino dei sistemi, nel comune interesse delle strutture coinvolte e dei cittadini stessi", continua Romano -. Pertanto, si ribadisce, la Asl1 non ha mai potuto conoscere dettagli inerenti presunte trattative, regole di ingaggio, metodi di pagamento o valori di riscatto. Di conseguenza, nessun soggetto esterno alla struttura può essere a conoscenza di tali dettagli".

Nella nota si entra nel merito degli attacchi e delle modalità che lo hanno provocato: "Al vaglio della task force, oltre alle operazioni di ripristino dei dati, anche le modalità attraverso le quali l'intromissione è avvenuta. Non è aspetto di second'ordine, infatti, che attacchi di tipo ransomware siano stati recentemente attuati anche nei confronti di svariate aziende sanitarie locali e regionali, per non parlare di istituzioni ed enti di cabotaggio nazionale e internazionale, segno di come l'emergenza contro cui la Asl1 e la Regione Abruzzo stanno combattendo sia pericolo comune e non circoscritto, oltre che innescabile presso qualsiasi struttura, da qui le estreme difficoltà e il conseguente impegnativo lavoro nel ricostruire la provenienza degli stessi".