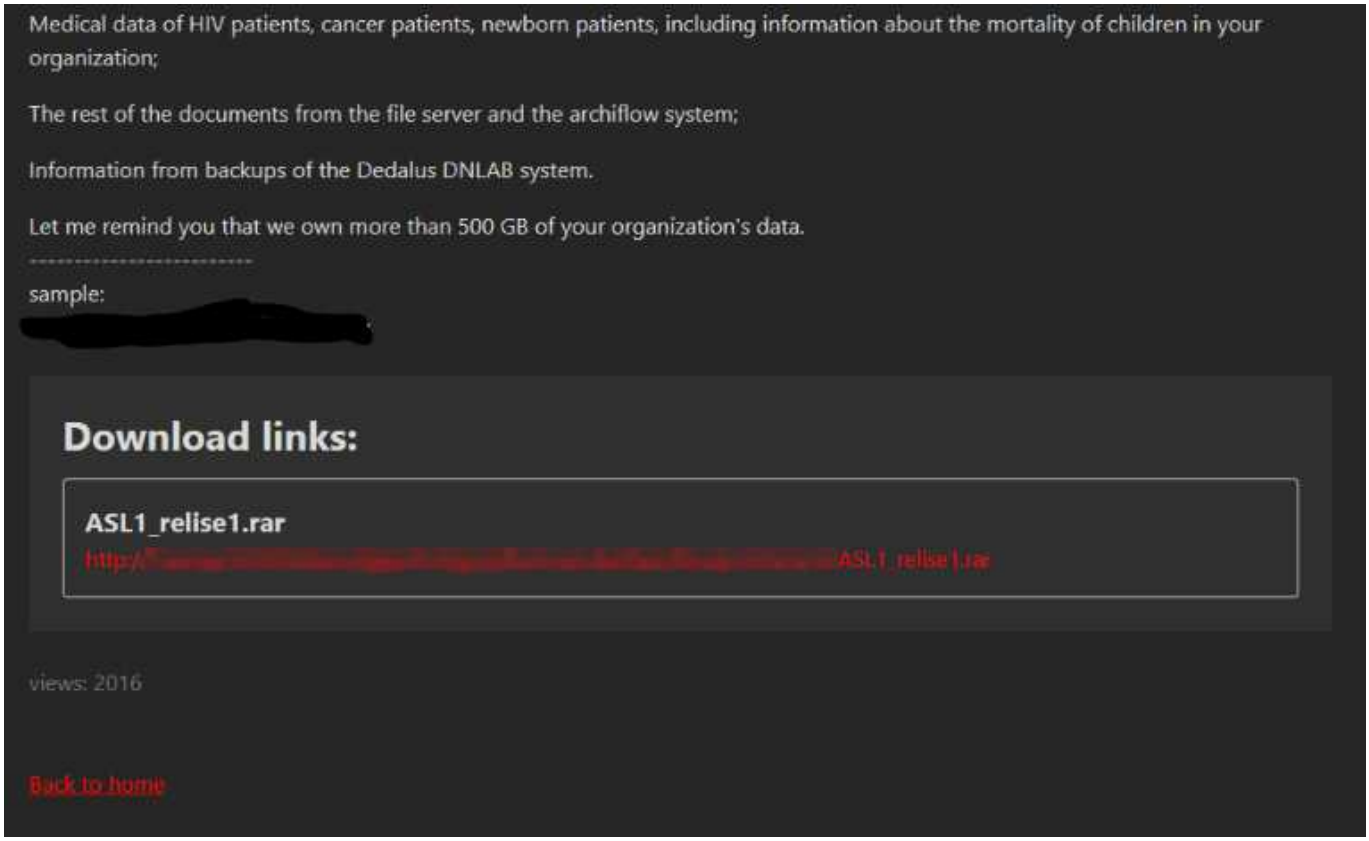
ASL L'AQUILA: PRIMI 10 GB DI DATI SENSIBILI NEL DARK WEB, CYBERGANG PASSA DA MINACCE AI FATTI

9 Maggio 2023



L'AQUILA – La cybergang Monti Ransomware passa dalle minacce ai fatti: con un aggiornamento della sua bacheca nel dark web, ha pubblicato un link che consente di scaricare a chiunque i primi 10 gigabyte degli oltre 500 gigabyte "trafugati" il 3 maggio dai server della Asl provinciale, dati sensibili, e coperti da privacy, referti e diagnosi di pazienti, anche con Hiv e oncologici, neonati, informazioni sulla mortalità infantile. Dati personali dei medici e dipendenti, compresi i dati bancari, informazioni amministrative e legali.

A rivelarlo è l'autorevole rivista online www.redhotcyber.com, che tratta temi di tecnologia e di sicurezza informatica, punto di riferimento per molti professionisti del settore, che ha pubblicato anche uno screen-shot della pagina dei criminali informatici, da cui è possibile effettuare il download.

Nei giorni scorsi gli hacker avevano chiesto un anticipo del riscatto, che potrebbe essere milionario, da versare in valuta digitale, dopo aver indicato le tempistiche con cui avrebbero poi, in mancanza di riscontro i dati sensibili, che potrebbero determinare pesantissime richieste di risarcimento danni da parte delle vittime nei confronti della stessa Asl, che è responsabile della custodia dei dati.

Alla Asl dell'Aquila è intanto corsa contro il tempo per attenuare i gravi disagi nelle prestazioni e nei servizi causati dall'attacco hacker subito il 3 maggio, dovuto all'inaccessibilità dei server.

I tecnici e i vertici, coordinati dal direttore generale, Ferdinando Romano, hanno costituito una task force "di pronto intervento di sicurezza informatica" che sta operando a supporto dei gruppi tecnici interni. Ci sono stati contatti con alcuni provider nel tentativo, stando a quanto emerso, di realizzare un nuovo sistema informatico. Però anche in questo caso l'ostacolo è il fattore tempo, e il ritorno alla normalità sembra lontano: nessuno fa previsioni, ma l'infrastruttura informatica potrebbe essere non funzionante per un mese.

E intanto continua il caos per utenti e pazienti. Non è ancora possibile effettuare la prenotazione di prestazioni a sportelli Cup, call center e servizio online. Tuttavia saranno garantite le prestazioni sanitarie già prenotate. Chi ha una prenotazione può presentarsi allo sportello Cyo per pagamento e registrazione del ticket nel giorno fissato per la prestazione con foglio di prenotazione ed impegnativa. Chi invece deve prenotare una prestazione urgente ovvero laddove sull'impegnativa sia presente la classe di priorità U può recarsi allo sportello Cup di un ospedale che contatterà il reparto interessato ai fini della erogazione della prestazione.

I dipendenti sono tornati alla carta e alla penna, e addirittura ai fax. I dati clinici e le comunicazioni varie vengono portate a mano, e non più condivise on line e inviate via mail, e le liste di attesa sono destinate ad allungarsi. In alcuni uffici i dipendenti sono stati messi in ferie forzate e in orari ridotti, visto che molte mansioni ammnistrative e di desk con carta e penna non possono essere svolte.

Gli stipendi saranno pagati regolarmente, comprensivi di indennità accessorie", ha però oggi rivelato la Uil, nella prima nota diramata a quasi una settimana dalla drammatica emergenza.

La Direzione aziendale "respinge con fermezza la divulgazione di notizie totalmente infondate e tanto più gravi in quanto tendono a colpire la credibilità della Asl in un momento delicato in cui la stessa è parte lesa di un vile attacco criminale, in ordine alla disinformazione di presunte carenze di antibiotici e di una operatività degli ospedali azzerata".

Intanto, un gruppo di medici ha lanciato l'allarme sulle conseguenze del possesso, da parte dei pirati informatici, dei dati bancari, tra cui gli iban dei dipendenti: "In banca siamo sicuri – spiega il gruppo di medici – che non ci possano essere pagamenti non dovuti, ma con questa disponibilità di dati si possono contrarre contratti di acquisto. È un'ulteriore spada di Damocle in una situazione dal punto di vista sanitario molto grave".

Scrive dunque www.redhotcyber.com: "Oggi Monti Ransomware effettua un ulteriore aggiornamento riportando che i primi 10GB di dati sono disponibili al download, come riportato nella print screen successiva. Il Data Leak Site (DLS) di Monti Ransomware non consente come altri gruppi ransomware di effettuare l'accesso ai dati direttamente attraverso un directory listing, ma viene messo a disposizione un file archivio di 10GB liberamente scaricabile online".

Il sito ricorda poi che "l'accesso alla rete onion e al download dei dati (attraverso TOR Browser) è praticabile da chiunque, anche se non dotato di particolari competenze in materia. Ciò significa che tali dati sono accessibili da qualsiasi persona che sappia normalmente utilizzare un PC".

E osserva: "la pubblicazione parziale di informazioni all'interno dei siti underground delle gang ransomware, sono anche un modo per aumentare la pressione verso l'azienda violata e quindi monetizzare, minacciando l'azienda della completa pubblicazione dei dati acquisiti forzandola a pagare il riscatto. Il ransomware sta sempre più diventando un minaccia per aziende pubbliche e private, dove in Italia sta dilagando mietendo vittime giorno dopo giorno. Il ransomware è un tipo di malware che cifra l'infrastruttura IT di una organizzazione rendendola inutilizzabile chiedendo un riscatto per poterla sbloccare minacciando la pubblicazione dei dati".

Infine viene riportato il contenuto della prima e minacciosa comunicazione degli hacker, di cui Abruzzoweb ha già riferito.

"Al momento, siamo pronti a pubblicare i seguenti dati nel nostro blog: dati personali dei dipendenti dell'organizzazione, compreso l'indirizzo del luogo di residenza, telefono, e-mail, codice fiscale; informazioni amministrative dalla sezione "Controllo Gestione"; dati legali, tra cui sentenze, protocolli, ecc. 15 documenti arbitrari (doc, xls, pdf) dal file server dell'organizzazione; 15 documenti arbitrari (pdf) entro il 2022 dal sistema archiflow".

"Inoltre, affinché non abbiate dubbi sul fatto che siamo proprietari dei dati medici dei vostri pazienti, pubblicheremo una parte dei documenti sul monitoraggio ambulatoriale della pressione arteriosa. Se i nostri requisiti non saranno soddisfatti, saremo costretti a pubblicare il resto dei dati medici sul monitoraggio ambulatoriale della pressione arteriosa, nonché i dati medici dei pazienti, comprese le diagnosi e le terapie prescritte, nelle aree di Fisiopatologia e Ostetricia, e altri 50 documenti arbitrari dal file server e dal sistema archiflow".

"Se anche in questo caso non si riuscirà a trovare un accordo, verranno pubblicati i seguenti dati: Dati medici di pazienti affetti da HIV, pazienti oncologici, pazienti neonati, comprese le informazioni sulla mortalità dei bambini nella vostra organizzazione; Il resto dei documenti del file server e del sistema archiflow; informazioni provenienti dai backup del sistema Dedalus DNLAB. Vi ricordo che possediamo più di 500 GB di dati della vostra organizzazione".

Sulla vicenda sono in corso due indagini: la prima della Procura aquilana e della Polizia postale sia del capoluogo ma anche di Roma, l'altra da parte dell'Agenzia nazionale per la Cybersicurezza. Occorre anche in particolare capire perché il sistema

antivirus, aggiornato un anno fa, si è rivelato con tutta evidenza inefficace, e aspetto dirimente è anche capire in che misura, se e quando, sono stati effettuati i back up dei dati sensibili.

ASL L'AQUILA: "NESSUNA CARENZA ANTIBIOTICI E NIENTE BLOCCO INTERVENTI"

La Direzione aziendale respinge con fermezza la divulgazione di notizie totalmente infondate e tanto più gravi in quanto tendono a colpire la credibilità della Asl in un momento delicato in cui la stessa è parte lesa di un vile attacco criminale." Lo si legge in una nota aziendale a fronte dell'attacco hacker che, tra gli altri effetti nefasti sta destando apprensione tra gli utenti.

E' questa la risposta dei vertici aziendali della Asl dell'Aquila, in ordine "alla disinformazione di presunte carenze di antibiotici e di una operatività degli ospedali azzerata", nel pieno dell'emergenza attacco hacker.

"Nonostante l'emergenza in corso, continua la Direzione Aziendale, tutto il personale dell'Azienda si sta prodigando per mitigare i disagi a pazienti ed utenti, permettendo l'esecuzione completa dell'attività chirurgica programmata e urgente. Nessun intervento chirurgico programmato ordinario e in Day-Surgery risulta essere stato annullato." La conferma arriva anche dal Responsabile del Blocco Operatorio Dott. Luigi Panella che dichiara "le voci inerenti un blocco o rallentamento dell'attività chirurgica programmata, che procede con i consueti ritmi, sono prive di fondamento. Anche l'attività di preospedalizzazione procede regolarmente per quanto attiene le visite anestesiologiche programmate, con il limite in alcuni casi di un rinvio temporaneo dei prelievi ematici per non sovraccaricare l'attività del laboratorio analisi".

Interviene anche il direttore del Servizio Aziendale del Farmaco, dott.ssa Esther Liberatore che chiarisce "allo stato evidenziamo che non risultano carenze di farmaci e di antibiotici. In particolare, per quanto riguarda gli antibiotici, le giacenze e le tipologie presenti nei magazzini farmaceutici aziendali consentono di coprire l'intero spettro di azione di queste molecole."

"Il Servizio Aziendale del Farmaco, inoltre, ha provveduto a contattare le ditte fornitrici che si sono rese disponibili all'invio dei farmaci con la modalità del conto anticipo e nella giornata odierna, dopo aver effettuato un controllo capillare delle giacenze nei quattro magazzini farmaceutici della Asl, si è già inviato il fabbisogno mensile alle ditte farmaceutiche."

FEDELE: "UN DISASTRO, DA CENTRODESTRA TIMIDE DICHIARAZIONI IN POLITICHESE"

Sulla pubblicazione dei dati sensibili interviene il Consigliere regionale del Movimento 5 Stelle Giorgio Fedele che già il 4 maggio denunciò la prima pubblicazione di un referto sulle pagine deep web del gruppo Monti.

"Sarebbero solo la prima tranche dei dati rubati dai data base dell'Azienda sanitaria abruzzese – continua Fedele – la Asl 1 ha subito una violazione senza precedenti nella nostra regione. Si conferma la gravità del caso, come del resto sto denunciando da tempo: il primo referto che ho portato io stesso all'attenzione delle istituzioni, dei cittadini e della stampa risale al 4 maggio. Oggi, a distanza di 6 giorni dalla prima denuncia che ha confermato l'esportazione dei dati, dobbiamo sentire ancora il Presidente della Regione parlare di riserbo per lo svolgersi delle indagini, o di attacco in corso. Caro Presidente se non se ne fosse accorto l'attacco Hacker non è in corso, ma è stato già fatto e i dati sono in mano a dei criminali, i servizi sono fermi, il personale è messo in ginocchio. Non ci sono indagini che richiedono il riserbo – incalza Fedele – c'è la necessità di un Presidente che prenda le redini della situazione, dimostri vicinanza agli operatori sanitari e ai cittadini, e faccia tutto quanto possibile per uscire da questa drammatica spirale. Non c'è certo bisogno di chi minimizza il problema".

"Questo è un disastro riconosciuti da tutti, e a questo proposito voglio ringraziare i colleghi dell'opposizione di centrosinistra che si sono interessati alla vicenda e che si sono uniti al Movimento 5 Stelle in questa battaglia per la verità. Nella commissione sanità prevista per le ore 15 di oggi pomeriggio, come Movimento 5 Stelle, abbiamo chiesto di inserire un ulteriore punto all'Odg per ascoltare sulla questione il presidente Marsilio, l'assessore alla Salute Nicoletta Verì, il direttore della Asl 1 Ferdinando Romano e dei responsabili per la tutela della privacy e dei sistemi informativi. Purtroppo, a quanto abbiamo appreso dalla convocazione, sarà in aula solo il direttore Romano. Il centrodestra continua a tacere o a esprimersi con timide dichiarazioni in politichese. Intanto nel dark web ci sono i dati degli abruzzesi che potrebbero essere venduti al miglior offerente" conclude".

GINNETTI UIL FPL "GLI STIPENDI SARANNO REGOLARMENTE PAGATI"

"Gli stipendi saranno pagati regolarmente, comprensivi di indennità accessorie".

Il segretario provinciale della Uil Fpl Antonio Ginnetti, il responsabile Sanità Uil Fpl Gianfranco Giorgi e il componente di segreteria Uil Fpl Claudio Incorvati rassicurano sull'erogazione degli stipendi dei dipendenti della Asl aquilana, che non sono quindi a rischio, nonostante il grave attacco hacker subito negli ultimi giorni dal sistema informatico dell'azienda sanitaria.

"Abbiamo avuto contatti con il management aziendale e ci è stato assicurato che gli stipendi sono in erogazione – affermano – Abbiamo inoltre avuto rassicurazioni anche sulle indennità. Ci è stato inoltre ribadito che il gruppo di pronto intervento di sicurezza informatica, a supporto dei tecnici dell'azienda, sta lavorando ininterrottamente con il coordinamento della direzione strategica".

Per quanto riguarda il servizio all'utenza, inoltre, la Uil Fpl precisa di essere in attesa di avere ulteriori dettagli: "Abbiamo ricevuto tante segnalazioni da parte degli utenti sulle problematiche relative ai servizi. Siamo per questo, e anche per la questione degli stipendi dei dipendenti, in costante contatto con la dirigenza aziendale. In questo momento per i servizi si stanno attuando delle procedure alternative per cercare di riportare la situazione alla normalità il prima possibile. La vicenda è molto delicata e, dal canto nostro, possiamo garantire che monitoreremo la situazione fino alla sua completa risoluzione".

© 2026 Abruzzo Web Enfasi srl - Quotidiano digitale registrato presso il Tribunale dell'Aquila con decreto n°501 del 2 settembre 2003
Iscrizione al ROC n. 26362 - P.IVA 01812420667
Direttore responsabile Berardo Santilli