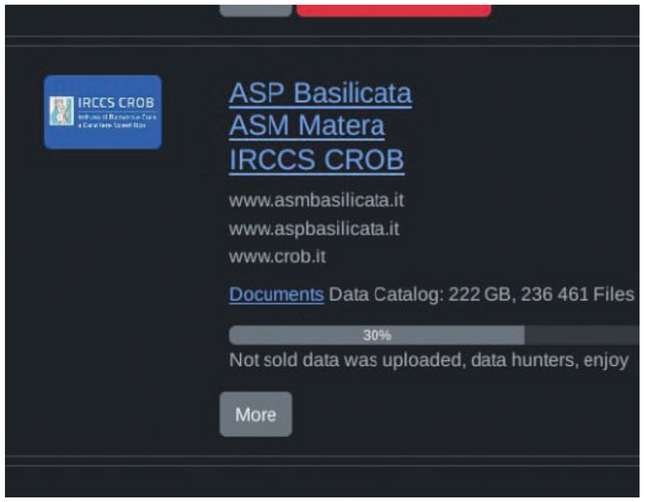
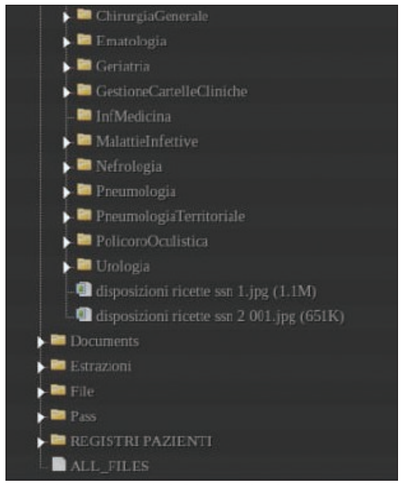
L'INTERVISTA

L'esperto Liuzzi e gli atti dell'ente sull'attacco hacker

La sede della Regione Basilicata e alcuni documenti di utenti lucani pubblicati sul dark web da Rhysida





Le sedi delle strutture sanitarie finite nel mirino dei cybercriminali: l'Asm di Matera e, sotto, la Asp Basilicata (a sinistra) e il Crob di Rionero

Dati rubati, i silenzi della Regione

Le mancate comunicazioni ai cittadini, i quesiti sulla sicurezza, le possibili conseguenze

di ROCCO PEZZANO

«Personalmente sono stanco di vedere la popolazione lucana trattata da "popolo ignorante" nutrito solo di sagre, tarantelle, vino rosso e peperoni cruschi. Per me è arrivato il momento di cambiare questa narrazione e continuerò nel mio piccolo a impegnarmi per questo»: lo sfogo è di Giuseppe Liuzzi, al termine di questa lunga intervista in cui il consulente freelance lucano nel settore della sicurezza informatica parla dell'attacco al sistema digitale della sanità lucana.

Nel corso dell'intervista Liuzzi – pur ferrato nel settore e capace di analizzare la vicenda dal punto di vista tecnico – punta il dito soprattutto contro l'assenza di trasparenza da parte della Regione Basilicata sul fatto in sé e su quanto fa per la sicurezza informatica.

Liuzzi – 33 anni, di Grassano – ha lavorato anche come formatore di "nuove tecnologie": industria 4.0 e fabbricazione digitale (stampa 3D). Ha fondato il Syskrack Lab nel 2014 e ad oggi coordina la sua comunità "glocale" di innovatori sparsa in Italia e nel mondo. Si definisce «fiero divulgatore della "consapevolezza" digitale».

Ha pubblicato nei giorni scorsi sul web un lungo testo in cui riporta le proprie impressioni – irte di tecnicismi per addetti ai lavori – sull'attacco del 28 gennaio scorso.

Lei ha studiato nel dettaglio l'attacco informatico alla sanità lucana. Vuole spiegarcelo in parole accessibili a tutti?

«Diciamo che ci ho provato, facendo ricerche e ricostruendo l'accaduto con l'aiuto di diversi professionisti, dopo ampio e accesso dibattito (ancora in corso). Purtroppo, come spiegherò più avanti, non sono state fornite molte informazioni riguardo l'attacco subito dagli enti coinvolti: Asp Basilicata, Asm Matera e Crob. Quel che son riuscito a fare riguardo agli "attaccanti" di Rhysida, dopo diverse settimane di ricerche, è raccogliere diverse informazioni nella rete, oltre a quelle "scucite" in giro, tra comunicati, post Linkedin e ciò che è stato pubblicato da alcuni blog di settore».

Chi o cosa è Rhysida?

«Rhysida è un "threat actor", "attore minaccioso", ossia qualcuno che può operare come un gruppo o un singolo. Pare sia una vera e propria organizzazione di cybercriminali che operano per il solo interesse economico dalle proprie operazioni o da quelle di altri "partner" e che già lo scorso 23 ottobre aveva colpito l'Azienda Ospedaliera Universitaria di Verona. Sembra si tratti dell'evoluzione di un precedente gruppo di cybercriminali col nome di "Vice Society". Rhysida utilizza un ransomware, un programma, in genere diffuso attraverso link via email o messaggi, in grado di contagiare altri sistemi nella stessa rete e che ha la caratteristica di "bloccare" l'accesso al sistema attaccato, prendendolo in ostaggio e chiedendone il riscatto. Rhysida è ancora più "particolare", poiché opera come un RaaS».

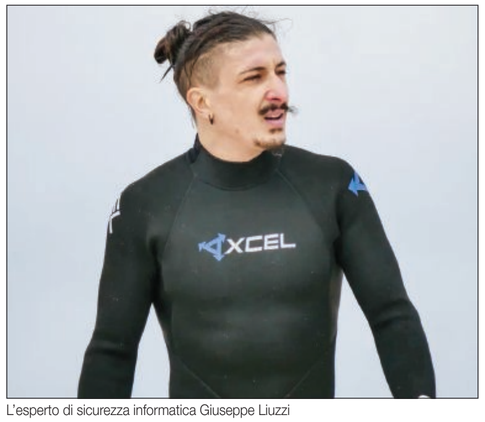
Che cos'è un RaaS?

«Un "Ransomware as a Service": fornisce su richiesta ad altri attaccanti il proprio strumento, come un'azienda fornisce il suo software ai suoi clienti e partner, mettendo poi a disposizione un vero e proprio portale, tipo un e-commerce, dove sono messi in vendita all'asta i dati sottratti agli utenti».

Fatte le premesse, partiamo dal principio?

«Lo faccio citando testualmente Nicola Mazzeo, responsabile del Sistema informativo lucano in un commento a un post pubblico su LinkedIn: "(…) L'attacco è stato fatto all'Asl di Matera e da lì, attraverso il Ris-Pacs, a tutte le altre Aziende del Servizio sanitario regionale. Roberto se n'è accorto ed abbiamo fatto subito la denuncia al Garante ed avvisato le altre aziende. Poi ci siamo resi conto che arrivavano da Matera. Se ingrandisci la foto ti accorgi che sono documenti su carta intestata di Matera. Comunque è ancora presto per capire cosa hanno fatto". L'articolo commentato riporta la data di pubblicazione del 24 febbraio, ma l'attacco dovrebbe essere iniziato diverse settimane prima visto che il primo comunicato dell'Asp riporta la data del 29 gennaio. Tuttavia la "kill-chain" (la catena di attacco) e le Ttp (tecniche, tattiche e procedure) solitamente utilizzate dall'attaccante sono ampiamente documentate da alcuni dei maggiori fornitori di servizi di sicurezza mondiali e andrebbero trattate per esteso e dettagliatamente, cosa qui impossibile».

> «Curioso il caso dell'asta per avere il riscatto bloccata da Rhysida»



L'esperto di sicurezza informatica Giuseppe Liuzzi

Prima di andare avanti, possiamo spiegare cosa sia un Ris-Pacs?

«Si tratta di due sistemi collegati da un software che permette il "dialogo" tra il Sistema informativo radiologico e il Sistema di archiviazione e trasmissione di immagini. Questi programmi o piattaforme consentono di tracciare ogni passaggio del paziente all'interno del poliambulatorio o dell'ospedale, per raccogliere tutti i documenti amministrativi e sanitari che lo riguardano e velocizzare l'intero processo radiodiagnostico. Successivamente, non ci saranno altre comunicazioni da parte di Asp Potenza e nessuna da Asm Matera e Crob, nessun avviso sul sito e pare nessun avviso nemmeno agli utenti. Quel che quindi sappiamo è che gli attaccanti pare abbiano iniziato da Matera, attaccando il sistema Ris-Pacs».

Torniamo alla ricostruzione dei fatti.

«Successivamente all'attacco o meglio alla sua rilevazione, approssimativamente in data 28/29 gennaio 2024, è stato richiesto l'intervento degli esperti di Acn – Agenzia per la cybersicurezza nazionale. Il 10 febbraio, sul sito dell'Acn, è riportata la notizia del ripristino dei servizi grazie al Csirt - Computer security incident response team -, ma senza alcuna menzione ai dati esfiltrati e all'asta che Rhysida ha subito aperto in seguito. Solamente il 15 febbraio vediamo la prima notizia sul sito dell'Asm (successivamente aggiornata il 7 marzo come riportato), intitolata "Prime disposizioni a seguito della violazione dei dati personali", ma senza alcuna indicazione su quale tipo di dati sia stato trafugato».

> «Tanti scenari e speculazioni specie in vista delle elezioni»

È a questo punto che Rhysida mette le carte in tavola e cerca di vendere i dati?

«Sì. Immediatamente dopo l'attacco, Rhysida mette all'asta i dati di Asm, Asp e Crob con un conto alla rovescia al termine del quale i dati saranno resi pubblici. Si parla di 900 gigabyte di dati, di certo non pochi. Con una buona probabilità, trattandosi di aziende ospedaliere, si parla di "Personal Health Information", cioè informazioni che permettono di identificare univocamente a livello globale una persona, con annesse informazioni strettamente personali sulle condizioni di salute. Riscatto fissato a 15 bitcoin. Con le oscillazioni di mercato bitcoin/euro siamo oggi a oltre 800.000 euro».

Questo attacco ha una peculiarità tutta sua: l'epilogo. Ce ne parla?

«L'attore minaccioso è solito operare con l'unico scopo di monetizzare. Usualmente, dopo l'esfiltrazione dei dati, passa alla fase del "ricatto": pubblica sul suo portale nel "dark web" (il web non indicizzato dai motori di ricerca) un conto alla rovescia, tempo entro cui il bersaglio colpito può pagare ed evitare che i dati vengano pubblicati online e liberamente scaricati da chiunque. Abbiamo seguito costantemente il countdown e la cosa curiosa è che al termine del countdown, i dati prima sono stati pubblicati (o almeno così sembrava, io non sono riuscito ad accedervi) e subito dopo invece l'asta è risultata "Temporary locked"».

"Temporaneamente bloccata": dunque un comportamento insolito per Rhysida.

«La cosa ancora più curiosa è che l'attore non si è di certo fermato nel corso degli ultimi mesi, continuando a tamburo battente a colpire enti e aziende di ogni parte del globo. Il tutto sempre con lo stesso iter e lo stesso ritmo, senza esitazione».

Poi, un nuovo colpo di scena qualche giorno fa.

«Già. Il 26 aprile abbiamo trovato i dati pubblicati online da Rhysida. Il 30 per cento, 220 gb circa di dati liberamente scaricabili».

Cosa può voler dire questa vicenda?

«Ovviamente questo curioso episodio, soprattutto in clima elettorale, ha dato vita a diversi scenari e speculazioni: "Perché tutto questo tempo e perché solo noi? Qualcuno stava pagando? Chi è il benefattore? Staranno attendendo il tempo di validazione della transazione in blockchain? Cosa c'era di così importante da valere così tanti soldi?". E questo si somma a tutta un'altra serie di domande a cui nessuno ha provveduto a rispondere nemmeno per tranquillizzare i cittadini, le vere vittime di tutto questo».

Assodato che la sicurezza assoluta nei confronti dei crimini informatici non esiste, cosa si può fare per limitare al massimo i rischi?

«Un dispositivo sicuro è spento, smontato e chiuso a chiave in uno scantinato. Nella sicurezza informatica i pilastri sono 3: Persone, Processi e Tecnologie e trascurarne anche uno solo vuol dire compromettere tutto il resto. Quel che secondo me fa la differenza è sempre e solo la consapevolezza, frutto di aggiornamenti, formazione, audit e simulazioni continue. Sensibilizzare i dipendenti, il personale ospedaliero, la dirigenza e tutte le persone coinvolte attraverso formazione continua oltre che tutta una serie di pratiche che ad oggi sono regolamentate e che aiutano tantissimo a trovare le falle, a chiuderle o mitigarle prima che qualcun altro lo faccia scatenando un incidente».

Facciamo qualche esempio?

«I "test di penetrazione" (penetration testing): si prova letteralmente ad attaccare il sistema, simulando il comportamento e le diverse prospettive dell'attaccante, ingaggiando talvolta anche il personale in vere e proprie simulazioni di attacco, proprio come le esercitazioni in caso di incendio o terremoto, ma molto più reali».

> «Nessuno ha dato conforto agli utenti, serve trasparenza e informazione»

Altre attività?

«I piani di gestione degli incidenti tra cui gli Incident response plan, ad esempio, che forniscono istruzioni sufficientemente dettagliate su come riconoscere e gestire gli eventi. Oppure i sistemi di Dlp, Data-loss prevention, che se accuratamente configurati aiutano a bloccare i tentativi di esfiltrazione dei dati da parte di un'attaccante. Ma di attività ne esistono tante: impossibile nominarle e descriverle tutte qua».

Un piccolo elenco di consigli pratici quotidiani?

«Partirei dalle cose più semplici ed efficaci: usare password lunghe, sicure e cambiate di frequente; aggiornare spesso i propri sistemi operativi e applicativi; imparare a riconoscere email, sms e chiamate fasulle (studiando i principi analogici e digitali di autenticazione); applicare i principi della "zero trust": nessuna fiducia e autenticazione continua».

C'è a suo parere una responsabilità della pubblica amministrazione nella vulnerabilità del sistema? C'era qualcosa che avrebbe potuto fare prima e non ha fatto?

«Lascio il gioco dello scarica-barile alla dirigenza, al management, ai dipendenti, ai consulenti e ai fornitori coinvolti. A posteriori è troppo facile dire cosa poteva essere fatto. Quel che è innegabilmente mancato e manca tutt'oggi è una comunicazione tempestiva ed efficace, indice di una scarsa preparazione nella gestione degli incidenti (incident response) e della comunicazione di crisi. L'abbiamo detto prima: nessuno è realmente al sicuro e gli attacchi saranno sempre più duri, difficili da riconoscere e frequenti. Quel che fa la differenza è come viene gestito un incidente e come viene comunicato all'interno e all'esterno, secondo trasparenza, dando risposte concrete e adottando un linguaggio responsabile e confortante agli utenti».

Cosa avrebbero dovuto fare secondo lei la Regione e le autorità sanitarie una volta accertato il furto d'informazioni riguardanti i cittadini?

«L'iter è definito dal Gdpr, il regolamento europeo sulla privacy, agli articoli 33 e 34. L'articolo 33 riporta chiaramente l'obbligo di notifica da parte del titolare del trattamento dei dati al Garante tassativamente entro 72 ore dal momento in cui è venuto a conoscenza della violazione. Contrariamente a quanto è facile reperire dalle ricerche online l'art. 34, dopo un ampio dibattito e approfondita lettura del Regolamento, è invece leggermente più "libero"».

In che senso? Cosa prevede?

«Nel senso che non riporta esplicitamente il tempo entro cui gli utenti, i diretti interessati e colpiti dall'attacco, devono essere contattati».

E quindi?

«Quel che mi piacerebbe sapere è appunto cosa è stato comunicato al Gdpr e se almeno qualche utente è stato avvisato, perché vista così come l'ho vista io e diversi professionisti del mio network, è sembrato l'ennesimo insabbiamento in vista poi delle elezioni appena concluse. Qualche comunicato in più sui siti istituzionali, sui portali regionali e soprattutto email ed sms di informazione agli utenti sarebbero opportuni. Nessuno ha pensato alle reali conseguenze di questo "data leak"».

Quali potrebbero essere queste conseguenze?

«Se i criminali sono in possesso di informazioni così sensibili – reperibili da documenti d'identità, passaporti o altri documenti strettamente confidenziali – possono abbonarti a qualsiasi servizio a pagamento, rubare totalmente l'identità di una persona, utilizzare la sua firma, il suo documento per una prenotazione in albergo, o anche semplicemente per aiutare i contraffattori ad avere database e informazioni sempre più accurate per la realizzazione di documenti falsi».

Come cittadino, ho diritto a conoscere quali siano le informazioni a disposizione dell'autorità pubblica, sanitaria o meno, e a sapere se siano finite nelle mani di qualcun altro?

«Io direi, chiaramente: "Sì". La lettura e lo scopo di una normativa così "utente-centrica" come il Gdpr non nasce per fare dei sottili giochi politici o di management, ma per ridare invece i diritti agli utenti. I dati a oggi rappresentano la più grande risorsa, maggiore del petrolio o di qualsiasi altro materiale e se ad alcuni ancora non è chiaro, beh, gli consiglierei di studiare un po' visto che le maggiori aziende e potenze mondiali basano i loro sistemi sulla raccolta di dati utente (Google, Amazon eccetera)».

Cosa suggerirebbe alla sanità lucana e all'amministrazione regionale per prepararsi a eventuali futuri attacchi informatici?

«Tutte le pubbliche amministrazioni devono rispettare le misure di sicurezza imposte da Agid, Agenzia per l'Italia digitale, che però non impone nulla di specifico se non "misure adeguate al contesto". Tuttavia nel contesto ospedaliero si parla di "Informazioni personali sulla salute", classificate come dati con regole speciali. Non sono semplicemente dati sensibili, ma esistono leggi e regolamenti specifici che stabiliscono come devono essere trattati e protetti. Sarebbe il caso pertanto di adottare standard e procedure di sicurezza adeguate alle tipologie di dati e sistemi che si vuole proteggere».

> «Ecco cosa fare per limitare i danni e difendere dati così sensibili»

Un esempio di standard?

«Basterebbe iniziare da quelli di alcune delle più conosciute certificazioni, per esempio la Iso 27001 o la normativa Nis 2».

Ci sono altri aspetti su cui ha rilevato poca trasparenza?

«Mi piacerebbe sapere: quali sono le figure coinvolte nella sicurezza dei sistemi? Esistono Ciso (Chief information security officer), Cto (Chief technology officer), Incident manager e altre figure importanti? Esiste un Soc (Security operations center), il centro di comando per la sicurezza informatica ospedaliera e regionale? Esistono i piani di gestione della sicurezza informatica? Esistono gli Irp (Incident response plan), i Bcp (Business continuity plan) o l'Information security plan? Esistono procedure per la gestione e la mitigazione del rischio? Come e dove vengono conservati e consultati i log (ossia le registrazioni sequenziali delle operazioni effettuate da un sistema informatico)? Vengono adottati adeguati e ben configurati sistemi di protezione, tra cui Edr, Intrusion detection system e Dlp? Già sapere quali siano gli sforzi messi in atto giornalmente rispondendo ad alcune di queste domande sarebbe opportuno per poter suggerire alcune azioni da intraprendere».

Tutte domande da girare alla Regione Basilicata. Altri aspetti da approfondire?

«Come ho già detto, la parte più importante è la consapevolezza: tutti noi dovremmo iniziare a conoscere rischi, opportunità e minacce reali legate al mondo della sicurezza. Visto soprattutto che in un modo o nell'altro siamo tutti coinvolti. È arrivato il momento di rompere quella percezione della cybersecurity o sicurezza informatica come "materia difficile" e complessa per poterla ignorare lasciandola solo agli esperti del settore, hacker con il cappuccio in testa o amministratori di rete a cui la testa va tagliata».