Cyber-AntiSec 2023

Rapporto di sicurezza

Redatto da

Edoardo Limone

SOMMARIO

INDICE DELLE FIGURE

GENERALITÀ

INTRODUZIONE

Il Cyber-AntiSec 2023 è stato rinnovato dal punto di vista “editoriale”: tra le modifiche eseguite è stato “pareggiato” il titolo con l’anno oggetto di analisi al fine di evitare incomprensioni nella lettura del documento.

Il rapporto è stato “compattato” al fine di occupare meno pagine ed essere più facilmente leggibile sui supporti mobili. Ci sono meno interruzioni di pagina ma si è comunque fatto attenzione a preservare una corretta separazione degli argomenti. Sono stati ridotti gli indici, avvantaggiandosi di una maggior chiarezza editoriale.

È stato un lavoro complesso ma si spera sia apprezzato dal lettore, a cui è d’obbligo fare i ringraziamenti per la fiducia ed il tempo dedicato alla lettura del rapporto.

INFORMAZIONI SULLE FONTI DATI

I dati collezionati durante questi dodici mesi, hanno ricevuto un contributo fondamentale dalla piattaforma Ransomfeed. Senza questa piattaforma, che opera gratuitamente sotto lo stretto controllo dei suoi sviluppatori, non si avrebbero informazioni rilevanti sui data breach. La piattaforma acquisisce in automatico le informazioni sugli attacchi ransomware pubblicati da oltre 160 cybergang; ogni informazione acquisita e pubblicata da Ransomfeed è controllata ripetutamente dallo staff e questo rende le risultanze affidabili e di qualità (è un lavoro che viene svolto ossessivamente).

È importante precisare che i dati di Ransomfeed, per una scelta specifica dello staff, non tengono in considerazione quegli attacchi che, seppur denunciati dai quotidiani e dalle stesse aziende vittima dei ransomware, non sono stati rivendicati ufficialmente dalle stesse cybergang.

Per questo motivo sotto ogni grafico/tabella del presente report sarà menzionata la fonte a cui si fa riferimento: è una correttezza dovuta in primo luogo ai lettori, ma anche alla professionalità del Gruppo di Lavoro della piattaforma Ransomfeed. La piattaforma è un’iniziativa DRM (Dashboard Ransomware Monitor), nata proprio con l’intento di

studiare il fenomeno ransomware soprattutto in ambito nazionale ma non solo. A questo proposito, per esattezza, si riporta quanto pubblicato sul sito ufficiale.

> *La Dashboard Ransomware Monitor (DRM) è un servizio di monitoraggio dei gruppi ransomware; utilizzando l'attività di scraping, ovvero l'estrazione di dati da più siti web per mezzo di programmi software e la successiva strutturazione degli stessi, la DRM memorizza le rivendicazioni in un feed RSS permanente, disponibile per la libera consultazione. Il servizio di monitoraggio della Dashboard Ransomware Monitor (DRM) è gratuito, raccoglie e analizza costantemente i dati relativi agli attacchi ransomware a livello internazionale. La piattaforma è in grado di rilevare in modo tempestivo gli attacchi e analizzarne i pattern, mettendo i dati a disposizione di chiunque desideri comprendere l'entità e l'evoluzione degli attacchi informatici.*

Per maggiori informazioni in merito al progetto Ransomfeed si raccomanda di visitare il sito principale all'indirizzo internet[1] riportato nella nota a piè di pagina.

SPECIFICHE SUI NOMI

Da molti anni è in corso su Internet una discussione in merito alla nomenclatura corretta degli attori malevoli. Convenzionalmente si è stabilito il termine hacker(s) che tuttavia non è tecnicamente preciso. Il termine hacker in effetti ha un'altra accezione:

> *Esperto di programmazione e di reti telematiche che, perseguendo l'obiettivo di democratizzare l'accesso all'informazione e animato da princìpi etici, opera per aumentare i gradi di libertà di un sistema chiuso e insegnare ad altri come mantenerlo libero ed efficiente. (Fonte: Treccani)*

Non ha quindi una valenza direttamente negativa: per contrassegnare un attore illecito ci sarebbero terminologie come ad esempio: black hat hacker. Per convenzione, tuttavia, si manterrà la definizione hacker per indicare coloro che compiono azioni illecite mentre per le altre categorie si farà l'opportuna specifica.

[1] Fare riferimento a questo link: https://ransomfeed.it/index.php?page=corporate

Chiarimenti sulla "perdita" dei file

Nel 2023 c'è stata un'ampia discussione in merito al fatto che i file oggetto di violazione ransomware ma non esfiltrati, non possano essere considerati "persi". Alcune pubbliche amministrazioni, infatti, hanno pubblicato dei comunicati stampa post-data breach, sostenendo tale tesi basandosi sul fatto che i file non vengono considerati persi perché non sono stati trafugati e sono rimasti nel perimetro del sistema informatico originario.

Questa conclusione è sbagliata e se ne forniscono le dovute spiegazioni. Dagli anni '90 l'informatica attribuisce ai file almeno sei requisiti essenziali, tali requisiti prendono il nome di *esade parkeriana*. Il nome deriva dal professor Donn B. Parker che ha esteso la precedente triade CIA (Confidenzialità Integrità e Accessibilità) con altri tre attributi molto importanti. L'esade parkeriana, per l'appunto, consta di sei requisiti, quali:

1. Confidenzialità
2. Integrità
3. Accessibilità
4. Possesso/Controllo
5. Autenticità
6. Utilità

Durante un'infezione ransomware i file vengono irrimediabilmente cambiati in modo illecito, provocando quindi la perdita di autenticità e d'integrità: per tale ragione essi non solo non possono più essere considerati originali. Tanto è vero che provando a calcolare l'hash, ossia la firma elettronica dei file, si otterrebbe una stringa differente per il file oggetto di data breach, rispetto a quello originale. Ne consegue che il file modificato da un ransomware non può definirsi in alcun modo *originale* e *autentico.* La versione originale viene considerata a tutti gli effetti persa a seguito di un processo illecito di corruzione (o meglio definita perdita d'integrità).

L'esfiltrazione ha quindi ben poca importanza nella "perdita del file" che avviene indipendentemente da essa; l'esfiltrazione è in realtà un'aggravante del data breach. Il fatto che sui comunicati stampa di alcune pubbliche amministrazioni sia stato legato il possesso logico del file al concetto di perdita è, pertanto, da considerarsi errato sia dal punto di vista metodologico che tecnico.

La perdita di possesso dei file può essere risolta con il ripristino da un'unità di backup: ma bisogna fare alcune considerazioni in merito per comprendere meglio la questione.

1) Se il backup fosse stato fatto correttamente, il file ripristinato sarebbe, effettivamente, una copia identica dell'originale. Se il backup fosse stato fatto alterando il file originale, i codici hash non combacerebbero e ciò provocherebbe il ripristino di una copia non identica del file originale.
2) L'unità di backup non è un'unità di produzione: ne consegue che non può fungere da giustificativo contro la mancata perdita di possesso. L'unità di backup è una risorsa straordinaria a cui si accede in occasioni eccezionali. Le valutazioni sull'integrità ed il possesso dei file vanno eseguite sull'ambiente di produzione e, in aggiunta, su quelli di backup ma in modo distinto.
3) Parlare di "perdita temporanea" della proprietà/controllo del file ha senso unicamente se la si mette in relazione con i tempi di ripristino (RTO, RPO, etc…). In relazione ad un'esfiltrazione vi è una condivisione illecita del file che non può considerarsi "temporanea": ormai l'attore malevolo è in possesso dei file trafugati e ne può disporre come meglio crede.

INTRODUZIONE: GLI ATTACCHI NEL 2023

Il 2023 si è presentato da subito con un incremento medio degli attacchi rispetto all'anno precedente. Facendo un naturale confronto tra il 2021, il 2022 e il 2023 non si può non notare la differenza[2].

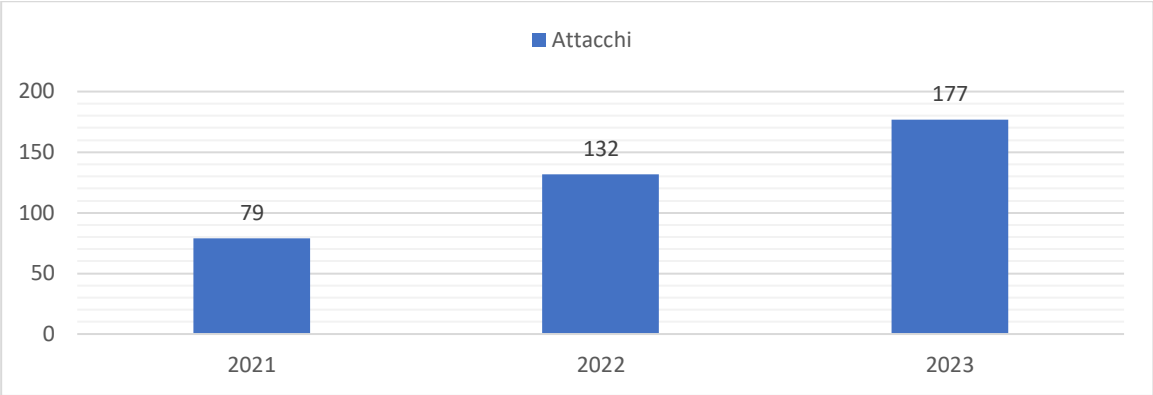

Figura 1 – Crescita degli attacchi tra il 2021 e il 2023

Vi è poi un aspetto che continua ad essere interessante, ossia la distribuzione geografica degli attacchi hacker; per facilitare la comprensione del fenomeno si è ristretta la rappresentazione alle prime cinque regioni più colpite.

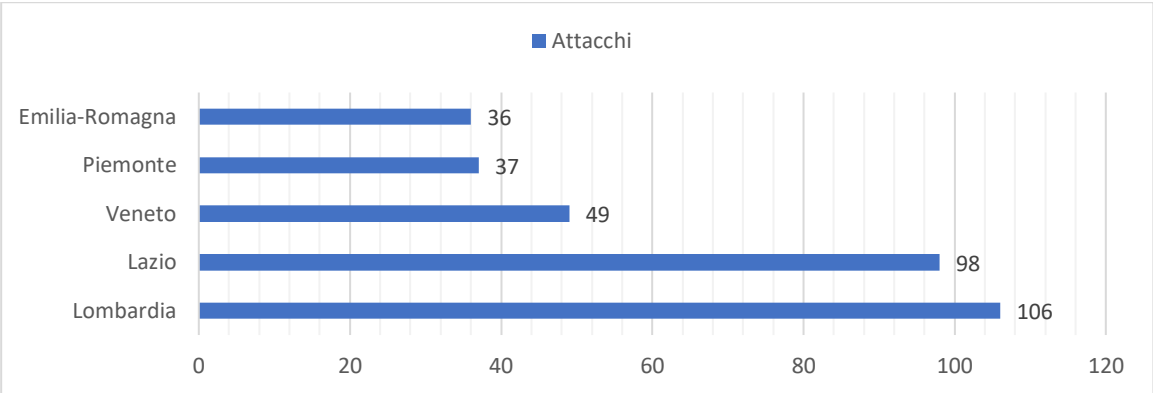

Figura 2 – Distribuzione geografica degli attacchi

Provando quindi a inserire queste regioni in un contesto di analisi che comprende solo gli ultimi tre anni, il grafico cambia come mostrato di seguito.

[2] Fonte: Ransomfeed ed EdoardoLimone.com

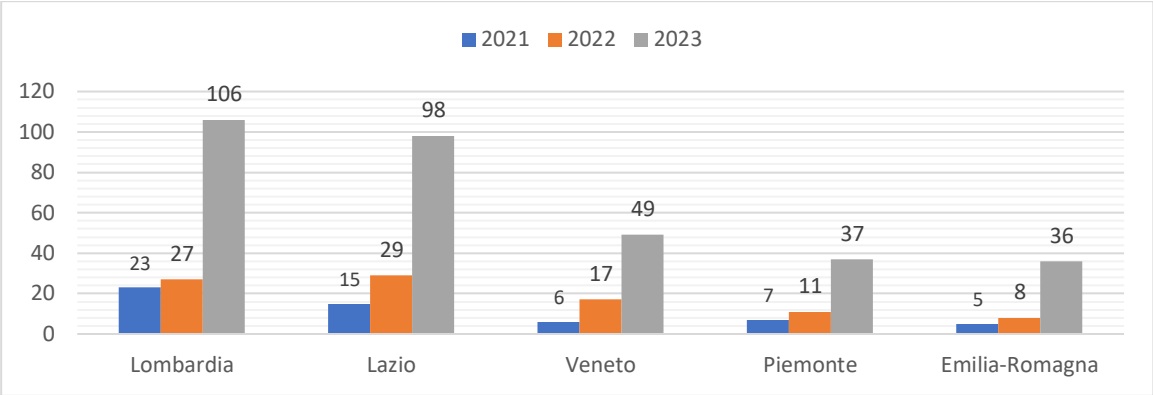

Figura 3 – Evoluzione temporale e geografica degli attacchi nelle regioni più colpite

A livello più complessivo, invece, quella che segue è la mappa delle occorrenze di attacco per ragione. Non si può fare a meno di notare che la massima concentrazione di attacchi è sulle regioni più ricche e sul Lazio, per definizione ritenuta la regione della pubblica amministrazione.

Figura 4 – Distribuzione degli attacchi su scala nazionale

Se si abbandonasse l'idea che tali risultati siano frutto del caso, ciò dimostrerebbe che gli attaccanti decidano consapevolmente i target da colpire o, quantomeno, la zona da colpire sulla base di un ragionamento prevalentemente economico. Ormai questo

dovrebbe essere un parametro assodato, benché molti analisti si ostinino a non tenerne conto.

Un altro aspetto più volte sottolineato è l'aumento della frequenza di attacco: si è passati da una frequenza[3] di attacco di 11 giorni del 2019, ad un attacco ogni 2 giorni nel 2023.

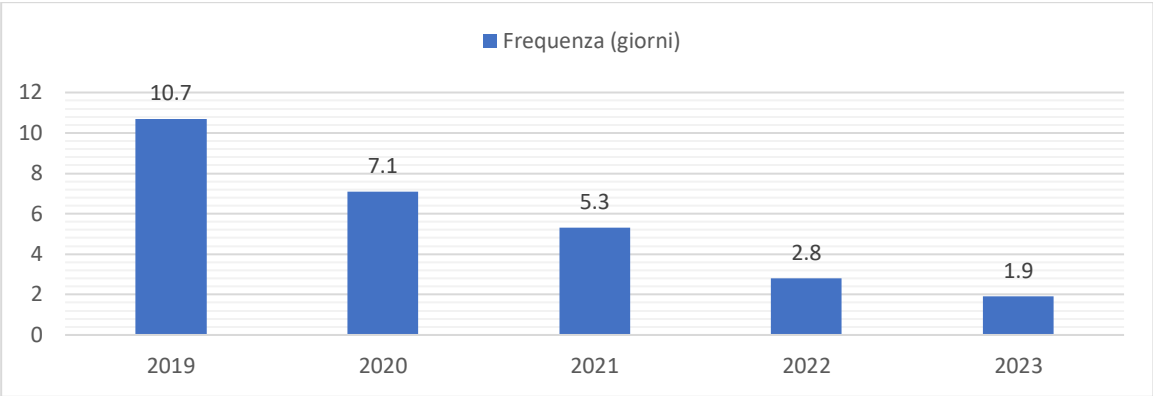

Figura 5 – Frequenza degli attacchi in giorni

RANSOMWARE E SANITÀ

Il 2023 è stato senza dubbio l'anno dei ransomware, minaccia davanti alla quale le organizzazioni private e gli enti pubblici hanno continuato a mostrarsi impreparati; il problema principale è stato l'impatto che questa tipologia di minaccia ha avuto sulla sanità. Ospedali, ambulatori, cliniche private, laboratori di analisi, una volta colpiti da ransomware hanno subito danni circa l'esposizione dei dati personali, soprattutto quelli di categoria particolare. Il caso più rilevante tra questi è stato, senza dubbio, quello della ASL 1 Avezzano-Sulmona-L'Aquila, accusata dagli assistiti di aver gestito male il data breach sia a livello tecnico che di comunicazione.

È doveroso menzionare anche il caso delle tre strutture sanitarie di Modena, colpite a fine anno: un attacco multiplo che apre una riflessione in merito a tutte quelle offensive che, colpendo un sistema unificato, impattano su più strutture moltiplicando i disagi, le conseguenze e i danni.

In ambito sanitario il Garante per la Protezione dei Dati Personali ha pubblicato un provvedimento[4] contro la ASL Napoli 3 Sud, oggetto di data breach nel 2022. La

[3] Fonte: EdoardoLimone.com
[4] Provvedimento del 28 settembre 2023, numero 426, documento web numero: 9941232, reperibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9941232

mancanza di misure di sicurezza come l'autenticazione a due fattori e una corretta segmentazione della rete interna attraverso l'uso di VLAN, sono state commentate all'interno del provvedimento. La multa comminata alla ASL Napoli 3 Sud è stata di 30.000 ma per la ASL1 Avezzano-Sulmona-L'Aquila la situazione potrebbe andare decisamente peggio. A maggio sono arrivate le richieste di risarcimento danni, ed erano solo le prime cento.


Attacco hacker alla Asl: arrivano le prime cento richieste di risarcimento danni

di Alessandra Ciciotti — 14 Maggio 2023

Figura 6 – Articolo pubblicato su Abruzzo Live

Se l'azione di denuncia e richiesta di risarcimento divenisse una procedura reiterata nei casi di data breach, la problematica della cybersecurity diventerebbe molto più sentita da parte delle aziende sanitarie. Si porrebbe comunque il tema dei risarcimenti: quando una ASL viene sanzionata, la multa comminata dall'Autorità è in realtà pagata con i soldi pubblici ossia con il denaro degli stessi cittadini. Anche per questo motivo il Garante è molto attento a non elevare troppo la multa che in tal modo, tuttavia, perde parte della sua funzione sanzionatoria. Il problema è che dietro molte inadeguatezze c'è una cattiva gestione dell'infrastruttura ICT, che non viene risolta certamente da una multa ma dovrebbe esserlo con la sostituzione della figura incompetente con una certamente appropriata: in sostanza l'azione del Garante non è direttamente connessa con quella necessaria alla risoluzione del problema.

Vi è infine da menzionare il caso della Azienda Ospedaliera Universitaria Integrata Verona a cui, a fine ottobre, sono stati sottratti 612 Gb su 29.000 Gb (0,6 Tb su 29). Graficamente la proporzione può essere rappresentata come segue e può indurre a pensare che le informazioni trafugate siano "poche" ma bisogna fare alcune riflessioni.

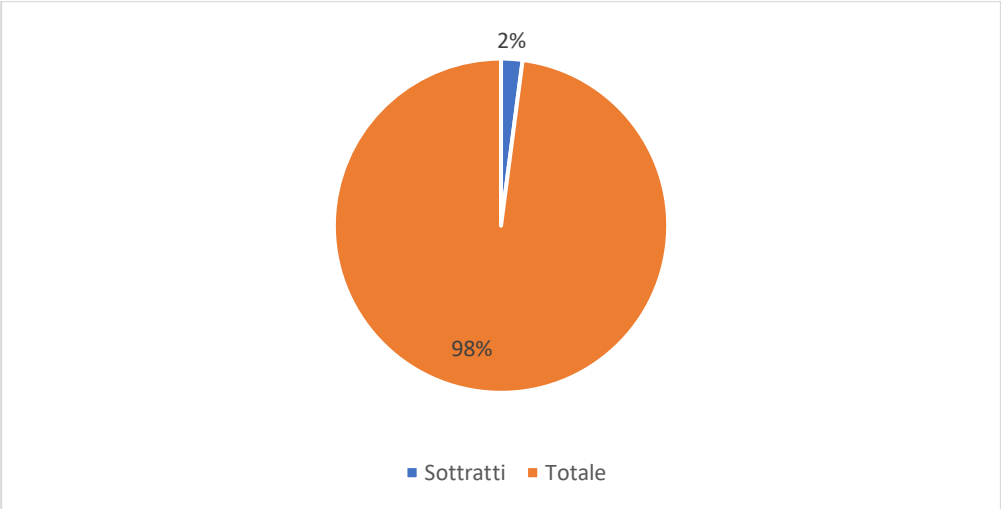

Figura 7 - Rappresentazione grafica dei dati sottratti alla Azienda Ospedaliera Universitaria Integrata Verona

La prima riflessione è che il totale dello spazio disco non può essere un indicatore rappresentante della gravità del data. A questo proposito nel comunicato ufficiale si legge:

> *Dalle verifiche sinora effettuate è emerso che i dati pubblicati rappresentano una minima parte di quelli complessivamente archiviati nei files server aziendali: 0,6 terabyte (pari a 612 GB) su 29 terabyte totali.*

Non è dato sapere, infatti, se tutti i 29 Tb fossero occupati. Se fossero tutti occupati la sottrazione sarebbe pari al 2% del patrimonio informativo effettivo. Ma se di 29 Tb fossero stati occupati 650Gb, ad esempio, e vi fosse stata la sottrazione di 612 Gb significherebbe una sottrazione di quasi il 100% del dati.

Una seconda riflessione riguarda le modalità con cui si tende a fare comunicazione. Un esempio è rappresentato dalla seguente frase:

> *La maggior parte di questi dati copiati risulterebbe essere non sanitaria, o addirittura già soggetta a pubblicazione per legge sul nostro sito web. I restanti dati, dei 612 GB copiati, rappresenterebbero documenti frammentari con informazioni cliniche, molte delle quali peraltro datate.*

L'utilizzo del "*peraltro*" sembrerebbe voler derubricare l'attacco e i suoi effetti. Il fatto che gli hacker non siano entrati in possesso di dati e informazioni aggiornate può ricondursi anche solo ad un caso fortuito ma, soprattutto, non costituisce giustificazione per un'eventuale e prorogata malagestione del dato.

Incapacità di ripristino

Gli incidenti degli ultimi anni sono stati contrassegnati da una fisiologica incapacità di ripristino nei tempi adeguati. Il grafico[5] seguente mostra la sospensione dell'operatività di alcuni soggetti colpiti negli ultimi mesi.

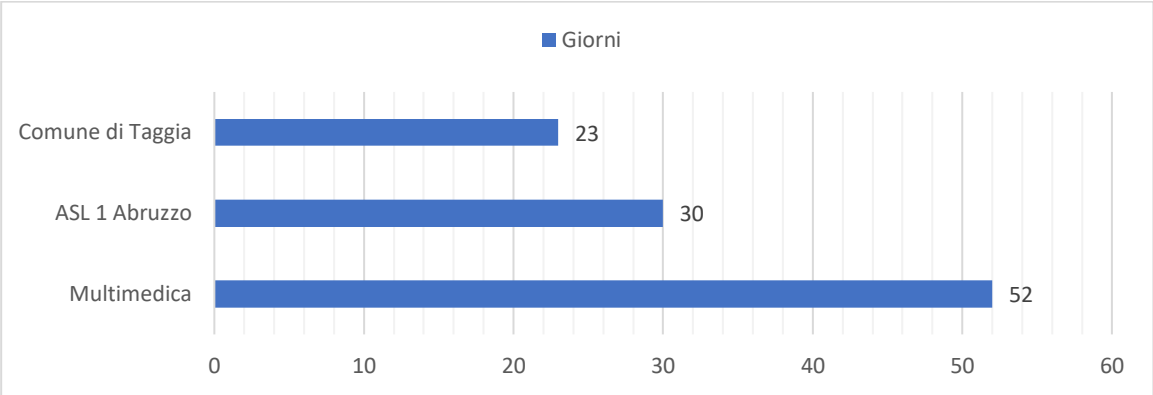

Figura 8 – Durata dei disservizi per alcuni soggetti colpiti da data breach

È palese che c'è una difficoltà nell'applicazione della capacità di *disaster recovery* e tale difficoltà risulta ancora più evidente se confrontiamo la durata del disservizio con quanto pubblicato sul portale AgID in merito al tempo di ripristino (RTO – Recovery Time Objective).

TIPOLOGIA	Numero Servizi in ambito	Numero Classi/servizi valutati	RPO minimo (h)	RPO Massimo (h)	RTO minimo (h)	RTO Massimo (h)
Università	21	14	8,26	60,87	12,29	87,27
Comune	22	9	28,09	45,32	37,81	73,47
Asl	26	6	16,42	70,95	11,71	91,16
Regione	95	10	0,67	120,00	3,00	136,00
Provincia	25	10	12,44	42,67	26,67	88,00

Figura 9 – Gli SLA di AgID suddivisi per tipologia di soggetto

È possibile notare che per le ASL il tempo massimo di disservizio è pari a 81,16 ore (ossia 3,7 giorni). Collezionare un ritardo di oltre trenta o cinquanta giorni, significa aver ecceduto gravemente il limite massimo raccolto da AgID. Questi dati sono stati acquisiti

[5] Fonte: EdoardoLimone.com

dall'Agenzia chiedendo alle P.A. di indicare il loro tempo minimo e massimo di RTO e RPO (Recovery Point Objective). Si tratta quindi di un dato fornito dalle stesse amministrazioni e non "imposto" dall'AgID.

Il problema riscontrato sugli SLA ha una spiegazione piuttosto semplice: i contratti di fornitura di beni e servizi non sono opportunamente definiti. Gli SLA devono essere oggetto di analisi e contrattazione e, quando non è possibile perché magari il fornitore è troppo importante e non si siede al tavolo delle trattative, è necessario sviluppare procedure parallele per tamponare eventuali carenze di fornitura. Inoltre, nei contratti continua spesso a comparire la clausola che offre al fornitore la libertà di gestire il tempo di disservizio rimanente, esponendo l'organizzazione al rischio di mancata operatività.

P.A. e Soggetti Privati

Il pensiero che la pubblica amministrazione sia meno solida della realtà privata è errato: innanzitutto per disponibilità di risorse, in secondo luogo perché molte delle funzioni della P.A. possono essere svolte da organizzazioni private che dimostrano di aderire alle misure minime di sicurezza di cui alla Circolare 2/2017 di AgID. Oggi vi è quindi una minore capacità di distingue tra pubblico e privato rispetto al passato.

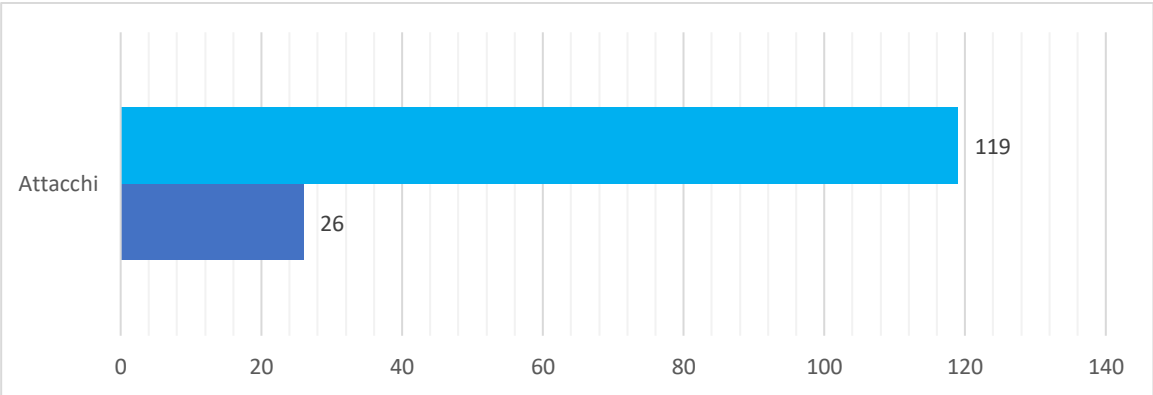

Figura 10 – Attacchi nel 2023 tra pubblico e privato

Ad esempio, attaccare un fornitore privato di servizi usati dal pubblico produce il medesimo effetto di attaccare il settore pubblico. D'altronde l'esperienza delle cosiddette in-house, le aziende che operano sul territorio ma che hanno una forma giuridica privata, sono inestimabili per la pubblica amministrazione. Il grafico, quindi, va interpretato nell'accezione corretta: lì dove si legge *privato*, bisognerebbe andare a verificare quante

realtà svolgono una funzione pubblica e si rimarrebbe stupiti dallo scoprire che non sono poi così poche.

GLI ATTORI MALEVOLI

L'analisi compiuta da Ransomfeed sugli attori malevoli tiene conto anche della fisiologica "movimentazione" dei gruppi: fusioni, scissioni, cambi di nome, sono tutti opportunamente tracciati. Il grafico[6] seguente mostra i principali gruppi che hanno agito nel 2023.

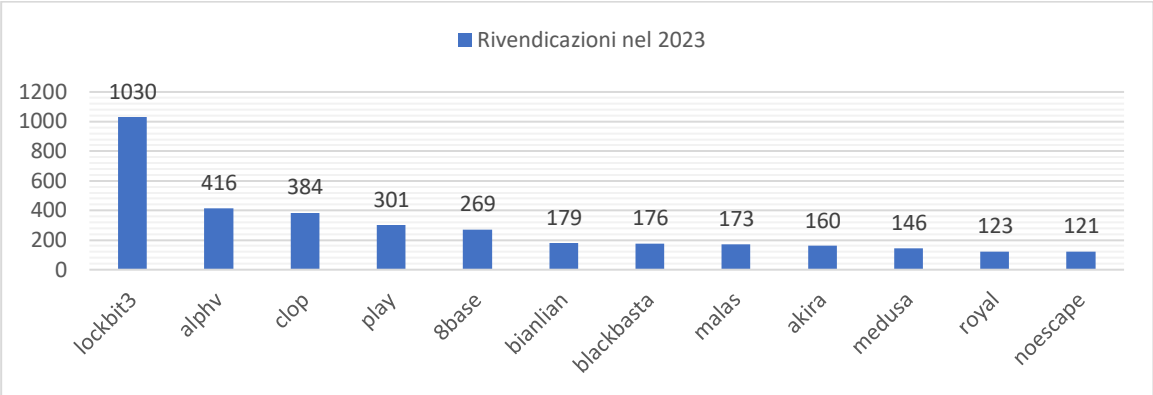

Figura 11 – Rivendicazioni degli attacchi da parte delle principali cybergang nel 2023

C'è da notare che, al di là dei numeri, l'attività operativa degli hacker è interessante anche per le collaborazioni estemporanee che possono stabilirsi tra i vari gruppi. Un caso[7] senza dubbio interessante è la "cessione di attività" da parte del collettivo RansomedVC che, dietro denaro, è disposto a cedere l'intera infrastruttura.

[6] Fonte: Ransomfeed
[7] Fonte: Ransomfeed

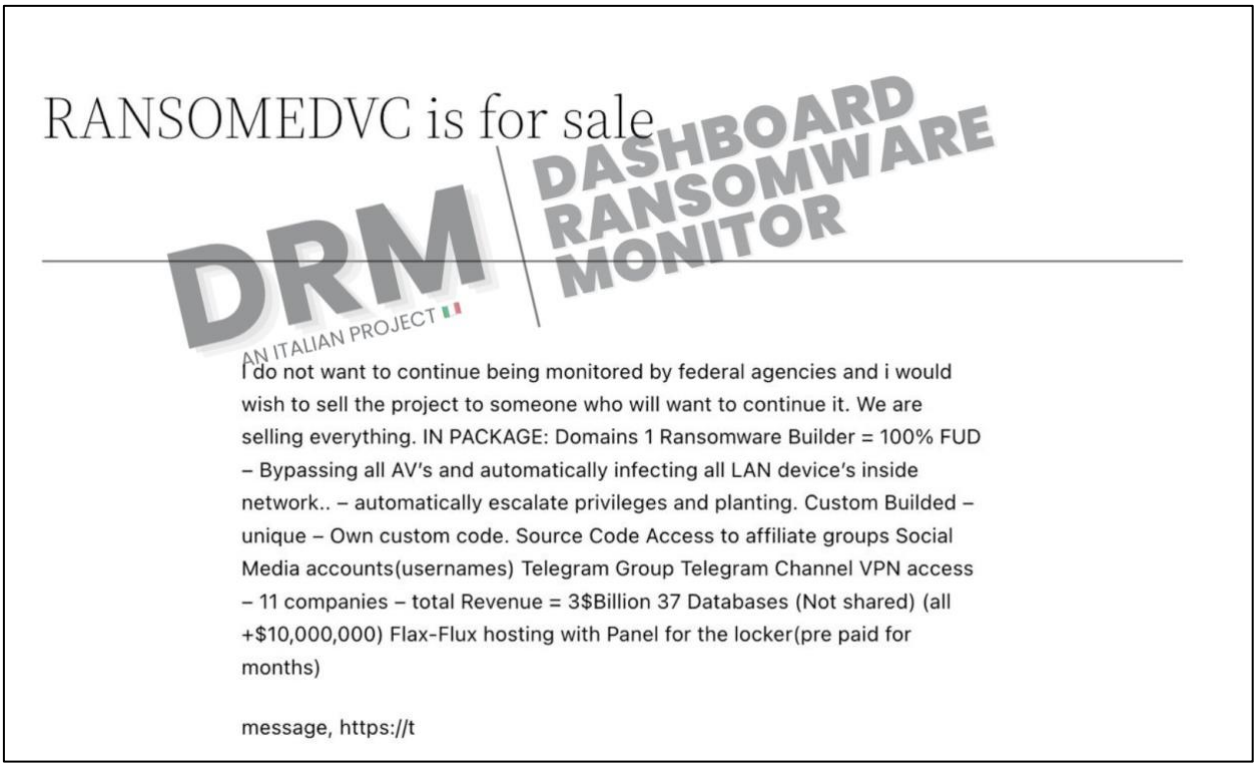

Figura 12 – Avviso di cessione attività da parte di RansomedVC

Queste "movimentazioni" dimostrano la natura delinquenziale delle cybergang che sono tutto fuorché disorganizzate nel loro business illecito.

La parte "sommersa" degli attacchi hacker

Come già detto all'inizio di questo rapporto, i numeri legati agli attacchi hacker dipendono dalle rivendicazioni pubblicate dagli hacker e dai comunicati stampa pubblicati online. Tuttavia, come è facile immaginare, vi è una numerosità di attacchi che resta "anonima" e "sommersa". A novembre 2023[8] c'è stato un convegno[9] a Cagliari intitolato "I***mprese artigiane e sicurezza informatica. Perché occuparsene, come gestire i rischi ed evitare gli attacchi***", i numeri presentati in quell'occasione sono così elevati da doverci far preoccupare. Nel 2022 si sarebbero registrati quasi 8.000 attacchi hacker ai danni di imprese e istituzioni

> *Nel 2022, secondo i dati elaborati dall'Ufficio Studi di Confartigianato Sardegna, le denunce alle Autorità di Pubblica Sicurezza, da parte di cittadini, imprese e*

[8] Per approfondimenti leggere l'articolo riportato cliccando qui.
[9] Annuncio ufficiale repereibile cliccando qui.

> *Istituzioni, relative agli attacchi hacker, sono state di 7.791, in crescita del +89,2% (media italiana 72,8% e quinto posto per l'Isola) rispetto al 2006, quando le segnalazioni furono solo 2.431 […] Tra le province italiane, al contrario, Cagliari è quella in Italia ha registrato più denunce per delitti informatici (truffe e frodi) da parte delle Forze di Polizia verso l'Autorità Giudiziaria: ben 95 segnalazioni ogni 10mila abitanti.*

Si tratta di numeri molto elevati, che in occasione del convegno furono presentati dalla Polizia Postale della Sardegna e pe precisione da Francesco Greco (Dirigente Centro Operativo sicurezza Cibernetica-Polizia postale Sardegna). Questi numeri meritano una riflessione, perché dimensionano ancora più criticamente il problema della sicurezza informatica ed il relativo rischio per le PMI.

Fenomeni autolesivi

I fenomeni autolesivi sono determinati da configurazioni volontariamente applicate dai tecnici e che risultano essere approssimative, negligenti, sbagliate, che producono danni al sistema informativo. Sono rappresentati anche da quell'insieme di comportamenti inaccettabili che vengono consentiti nell'infrastruttura informatica per "praticità", a danno della sicurezza e dell'integrità delle informazioni.

Credenziali esposte

In aggiunta ai rischi esterni a cui sono esposte le organizzazioni private e pubbliche, bisogna considerare quelli interni derivanti dalla negligenza e dalla mala gestione delle infrastrutture ICT. A distanza di anni continuano, ad esempio, a persistere i file di testo (*.txt) contenenti credenziali di accesso a sistemi, portali, servizi. La scelta delle password continua ad essere fatta sulla base della semplicità e della brevità, invece che sulla base della sicurezza. Restano assai rare le attivazioni spontanee di meccanismi di accesso multi-fattore che potrebbero invece ridurre sensibilmente le violazioni su portali e sistemi considerati critici.

Queste dinamiche non sono in alcun modo imputabili agli hacker, al contrario sono imputabili ad un atteggiamento autolesivo da parte di chi ha in gestione l'infrastruttura

informatica. Non sono nemmeno imputabili a costi di licenza, di dispositivi o quanto altro: la gestione sicura delle credenziali può essere, di fatto, eseguita mediante portachiavi cifrati con condivisione controllata nel gruppo di lavoro e il costo varia da pochi euro all'anno per utente, a zero euro quando la soluzione viene ospitata dalla stessa organizzazione.

Backup non sicuri

Poter eseguire correttamente un backup dovrebbe essere la base di qualsiasi infrastruttura informatica. Molte organizzazioni mantengono funzioni di backup mal configurate che, ad esempio, non sono dotate di versionamento. L'assenza di versioning produce, in molti casi, l'impossibilità di ripristinare i dati salvati ed espone i backup all'azione corruttiva dei malware. Inoltre, i servizi cloud che implementano il versionamento, raramente danno la possibilità di "cancellare" le vecchie versioni. Ciò tutela i dati anche da azioni dolose/colpose da parte degli stessi amministratori di sistema.

Inoltre, nella maggioranza dei casi esaminati, vi è l'assenza del backup in offline. Come è noto la regola del "3…2…1…Backup!" include il requisito che almeno un backup venga conservato in offline rispetto agli altri. Questo requisito è anche una misura minima di sicurezza, la 10.4.1:

> *Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.*

Quindi tale requisito, oltre ad essere una regola di buon senso, è anche un obbligo normativo per tutti i soggetti pubblici o privati che svolgono funzione pubblica. Ricordiamo che le misure minime di sicurezza si applicano ai soggetti rispondenti all'art. 2, comma 2 del C.A.D. (Codice dell'Amministrazione Digitale), ossia essenzialmente a:

1) **alle pubbliche amministrazioni** di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 […] ivi **comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione**;
2) **ai gestori di servizi pubblici**, ivi **comprese le società quotate**, in relazione ai servizi di pubblico interesse;

3) **alle società a controllo pubblico**, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b).

CONCLUSIONI

L'emorragia di dati sanitari fuoriusciti dai sistemi di ospedali, ambulatori, cliniche e quanto altro, denota la sostanziale incapacità di gestire dati particolari da parte di molti attori pubblici. Basta leggere il provvedimento del Garante precedentemente menzionato (28 settembre 2023 n.426) per capire la gravità della situazione.

> *gli utenti che si avvalevano della VPN erano circa 1200, che non era prevista una procedura di autenticazione a più fattori e che l'autenticazione veniva effettuata mediante le credenziali di dominio […] all'epoca dell'incidente di XX, non era attivo il meccanismo di password history per impedire il riutilizzo delle password […] l'Azienda al momento della violazione non disponeva di un piano di rispristino dei diversi servizi con particolare riguardo a quelli definiti "critici".*

La gestione di dati particolari da parte di attori non qualificati, negli anni passati (2022), ha esposto dati riguardanti abusi sessuali su minori ricoverati presso strutture pubbliche. Inutile ripetere il concetto espresso ormai fino allo stremo, ossia che la Circolare 2/2017 è obbligatoria dal 31/12/2017, ossia da ormai oltre, sei anni e che il fatto che molte pubbliche amministrazioni l'abbiano adottata solo in parte, dovrebbe far riflettere e probabilmente preoccupare. Si sta rivelando prezioso, invece, la conoscenza acquisita dalle aziende in-house sugli aspetti di cybersecurity e anche la sinergia che esse sviluppano con le piccole e medie realtà del territorio. Spesso queste iniziative creano filiere robuste atte a fronteggiare efficacemente gli incidenti.

NOTA DELL'AUTORE

Nel 2019 sedevo ad un tavolo di lavoro nel quale esprimevo grande perplessità sulla gestione della sicurezza informatica delle pubbliche amministrazioni. Intorno al tavolo c'erano DPO, tecnici, giuristi e alcuni di loro mi chiesero cosa muovesse le mie perplessità. La mia risposta spiegò che a preoccupare erano i dati provenienti da un osservatorio che avevo istituito qualche anno prima: i dati sono numeri, le evidenze derivanti da un data breach non sono opinabili. In quell'occasione alcune persone mi

fecero notare quanto poco ottimiste fossero le mie previsioni (come se lo scopo delle statistiche fosse garantire l'ottimismo e non la realtà). Replicai che andando avanti di questo passo ci sarebbe stata una reazione da parte dei cittadini, che fino a quel momento erano rimasti silenti ogni volta che i loro dati venivano sottratti. Il problema di tale reazione sarebbe stato legato all'eventuale risarcimento stabilito dal tribunale, che difficilmente sarebbe stato valutato con gli stessi criteri adottati dal Garante della Protezione dei Dati. Il Garante, infatti, sta ben attento a gestire l'importo sanzionatorio per non gravare sulle tasse dei contribuenti (che pagano la multa attraverso le imposte). Il tribunale, invece, accertato l'illecito, è sostanzialmente obbligato a deliberare un risarcimento ai danneggiati che rischia di essere anche piuttosto significativo.

Nel 2023 sedevo nel salotto del Direttore Generale di un'istituzione italiana: rappresentavo la preoccupazione verso il crescente numero degli attacchi, soprattutto in ambito sanitario. Presentai, anche in quell'occasione, i numeri, le statistiche, i dati aggiornati del medesimo osservatorio. Ripeto: parliamo di informazioni di natura *quantitativa*, supportati da fatti. La risposta fu "*Davvero? Non penso ci sia questa criticità in ambito cybersecurity sul fronte sanitario. Personalmente non la riscontro."* Ammetto che rimasi perplesso e, subito dopo, abbastanza sconfortato. È bastato aspettare: i data breach sono aumentati di numero, di frequenza, di complessità e i dati di categoria particolare (ad esempio i sanitari) sono diventati l'oggetto d'interesse degli hacker ma anche degli studi legali chiamati a proteggere i diritti degli interessati. A questo incremento si è sommata l'attività di protesta svolta dai cittadini nel caso della ASL1 Avezzano – Sulmona – L'Aquila, che dimostra quanto stia cambiando la cultura di massa in merito ai temi di trattamento dei dati personali.

Spiace rilevare che questo cambiamento debba passare per le azioni legali invece che per un'opportuna prevenzione; mi verrebbe da domandare oggi a quelle persone intorno al tavolo se sono ancora ottimiste. Fuori di polemica, lo scopo di questa breve nota è spiegare che, al di là delle opinioni personali legittime che ciascuno di noi può avere sull'andamento degli incidenti, i numeri non lasciano spazio a discussioni. Ogni ritardo, d'altro canto, verrà pagato amaramente direttamente sulla pelle dei cittadini. I numeri non danno spazio ad opinioni personali, i numeri non danno molto spazio nemmeno ad interpretazioni quando ben contestualizzati. I numeri non si valutano con la bilancia dell'ottimismo/pessimismo ma con la bilancia del "fare ciò che è necessario".

Spiace vedere una tale miopia soprattutto da parte di chi, quotidianamente, potrebbe fare la differenza nel Paese; spiace davvero tanto ma d'altronde i fatti non mentono. Il 29 novembre 2023 a Roma si è tenuta una conferenza organizzata dall'Associazione Difensori d'Ufficio. All'iniziativa hanno partecipato molti personaggi illustri, tra cui il capo della Polizia Postale Ivano Gabrielli che, in quell'occasione, ha fornito un dato interessante: entro il 2025 il valore economico dei danni causati da incidenti informatici di natura dolosa raggiungerà i 10 trilioni di dollari americani. La fonte di questa informazione, per esser precisi, è il "Directional Statement" dell'INTERPOL Secretary General Jürgen Stock", New Delhi, 2022, Pg. 4.

> *Experts estimate cyber-related crime to cause over 10 trillion US dollars in damages by 2025.*

Non è un problema iniziato ieri. Sono vent'anni che la criminalità organizzata sta evolvendo le sue attività illecite e negli ultimi dieci si è spostata sistematicamente sul dominio digitale. Non considerare i dati, ignorare le tendenze di attacco, derubricarne le conseguenze, non è solo miope ma è semplicemente da irresponsabili. Si spera che la cultura della prevenzione e della sicurezza, molto sottovalutata in Italia, possa un giorno diventare parte integrante della quotidianità di aziende pubbliche e private nel rispetto di quei principi che rendono l'Europa un continente in cui è desiderabile vivere e che ci ostiniamo a propugnare in convegni ed altri eventi.