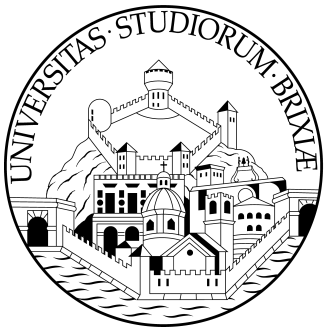
Elaborato di sicurezza informatica

Patrick Lorenzi

20 dicembre 2022



UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Indice

1 Introduzione

L'utilizzo di sistemi informativi in strutture sanitarie è aumentato negli ultimi anni, per far fronte ad esigenze di maggiore efficienza e flessibilità. Questo però aggiunge ai rischi già esistenti quello di un attacco informatico. Il panorama degli attacchi informatici è in continua evoluione, e le strutture sanitarie non sono esenti da tali attacchi.

Una tipologia particolare di attacchi sono quelli che utilizzano ransomware e wiper, malware che possono avere effetti distruttivi sui sistemi attaccati. Infatti, possono cifrare o cancellare i dati memorizzati nei sistemi, rendendo impossibile proseguire l'attività della struttura sanitaria, se non dopo un ripristino dei sistemi. Questa operazione però richiede tempo, durante il quale le attività della struttura sono più o meno ferme, con conseguenze per i pazienti.

L'approvazione del regolamento per la protezione dei dati nell'Unione europea (GDPR) introduce ulteriori norme da rispettare per quanto concerne la protezione dei dati personali. I dati sanitari sono una particolare categoria di dati personali, e le regole applicate per il loro trattamento sono più rigide rispetto agli altri.

Molti degli attacchi con wiper e, soprattutto, con ransomware vanno anche a rubare i dati resi inaccessibili. In generale, questo tipo di attacco va a colpire i dati personali dei pazienti, e ciò può comportare delle violazioni delle disposizioni del GDPR.

Questo documento si concentra su come attacchi ransomware e wiper possono causare danni ai sistemi delle strutture sanitarie, considerando anche l'aspetto della protezione dei dati, per poi illustrare le possibili contromisure per gestire il rischio portato da questi attacchi.

2 Background

2.1 Ransomware

Un ransomware (dall'inglese ransom, riscatto) è una tipologia di malware che impedisce ad un'organizzione di accedere ai propri dati, chiedendo un riscatto per ripristinare tale accesso. I ransomware documentati finora presentano un funzionamento simile tra loro: vengono individuati i file da cifrare (per esempio i file sotto la cartella Documenti), i file vengono cifrati utilizzando un algoritmo di cifratura e poi viene creato un file testuale sul desktop. Questo file spiega cosa è accaduto e come pagare il riscatto per ripristinare l'accesso ai file [1].

Nel corso degli anni, oltre ad effettuare quanto scritto sopra, i ransomware si sono evoluti andando a rubare i dati prima di cifrarli, la cosiddetta *doppia estorsione*. L'attaccante non solo rende inaccessibile i dati dei sistemi della vittima, ma li scarica anche su un proprio server, minacciando poi di rivelare pubblicamente i dati in caso di mancato pagamento di un riscatto, differente e aggiuntivo a quello da pagare per riottenere l'accesso ai propri dati [2].

Un ransomware è operato da un gruppo, talvolta chiamato anche *ransomware gang*. I ransomware utilizzati da gruppi diversi possono avere delle caratteristiche comuni, ma in generale differiscono per le vulnerabilità che sfruttano, il modo in cui cercando di espandersi nella rete infettata e il modo in cui vanno a cifrare i dati. Inoltre i vari gruppi hanno regole diverse sui possibili bersagli, con alcuni gruppi che scelgono vittime solo in alcune aree geografiche per esempio [3].

Un ransomware può essere utilizzato dal gruppo che lo ha creato, oppure anche da un affiliato, nel caso in cui l'operatore del malware lo renda accessibile ad altri. Quest'ultimo modello di business è anche chiamato Ransomware as a Service (RaaS) e permette ad un gruppo che opera un ransomware di effettuare molti più attacchi. Il gruppo offre il proprio ransomware in cambio dell'accesso a reti di aziende o istituzioni governative e di una percentuale dei ricavi dei riscatti, imponendo opzionalmente dei requisiti in termini di grandezza, località geografica o fatturato della vittima [4] [5].

2.2 Wiper

Un altra tipologia di malware che impedisce di accedere ai propri dati è il wiper (dall'inglese to wipe, pulire). A differenza del ransomware, questo va

a danneggiare permanentemente i dati, tipicamente andando a modificare alcune zone di memoria che vengono utilizzate dal sistema operativo per accedere ai dati. I wiper differiscono dai ransomware principalmente nel risultato ottenuto: utilizzando un wiper il sistema attaccato non può essere ripristinato nella maggior parte dei casi, mentre con un ransomware sì, dopo aver pagato un riscatto [6].

Un esempio abbastanza noto di wiper è NotPetya, un malware con capacità di propagazione (un worm) utilizzato per effettuari attacchi contro organizzazioni ucraine. Questo malware andava a cifrare i dati della vittima, senza però memorizzare la chiave utilizzata durante il processo, per poi chiedere alla vittima il pagamento del riscatto per riaccedere ai propri dati. Questo è un esempio di un wiper che finge di essere un ransomware, al fine di nascondere le reali motivazioni dietro l'attacco. In alcuni casi però è anche possibile che un ransomware implementi male la procedura di cifratura, rendendo impossibile riottenere i dati originali e diventando di fatto un wiper [7].

2.3 GDPR

Il regolamento generale sulla protezione dei dati (in sigla GDPR, dall'inglese General Data Protection Regulation), ufficialmente regolamento (UE) n. 2016/679, è un regolamento adottato dall'Unione europea il 27 aprile 2016. L'obiettivo di questo regolamento è di migliorare la protezione dei dati personali di cittadini dell'Unione europea (UE) e dei residenti nell'UE, sia per quanto concerne i dati memorizzati all'interno dei confini europei, sia per quelli esterni. Il GDPR impone delle regole stringenti su come devono essere trattati i dati personali dei cittadini, andando anche a richiedere la nomina di responsabili appositi all'interno dell'azienda, affinchè si occupino di gestire il trattamento dei dati personali. In caso di violazioni di queste regole sono previste delle multe, le quali sono calcolate sulla base del fatturato annuo dell'azienda o vengono forniti dei riferimenti nel caso di istituzioni pubbliche [8].

In particolare, questo regolamento fornisce anche la definizione di violazione dei dati personali (in inglese *data breach*), ovvero "una violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" [9]. I regolamenti in materia di privacy impongono alle aziende/istituzioni di notificare immedia-

tamente alle autorità (in Italia il Garante per la privacy) un data breach e, nel caso in cui ci possano essere conseguenze per i diritti delle vittime, di notificare anche le persone coinvolte tramite i canali appositi.

Per quanto detto prima un attacco ransomware può portare ad un data breach, in quanto un ente terzo non autorizzato (l'attaccante) accede ai dati presenti nel sistema, impedisce al personale autorizzato di accedere a tali dati e, nel caso di un attacco con doppia estorsione, procede anche a rubare i dati, minacciando di renderli pubblici.

3 Metodologia

In questa relazione sono considerati gli attacchi che hanno utilizzato ransomware e wiper contro strutture sanitarie, avvenuti negli ultimi cinque anni. Questi attacchi non sono gli unici che possono colpire una struttura sanitaria, ma possono causare un stop alle attività informatiche in assenza di adeguate procedure di ripristino. Per una struttura sanitaria un fermo dei sistemi di tale entità non può essere tollerabile, soprattutto in caso di emergenze.

La scelta del periodo è dovuta al fatto che attacchi di questo tipo sono diventati rilevanti in questo periodo, con un numero significativo di attacchi ransomware a partire dal 2016-2017. Il termine ransomware è diventato noto ai più a partire dal 2017, a seguito della diffusione del ransomware WannaCry.

Particolare attenzione viene prestata al periodo pandemico (2020-oggi), al fine di capire se c'è stato un aumento degli attacchi contro strutture sanitarie oppure no. L'ipotesi alla base di ciò è che le ransomware gang possano aver incrementato gli attacchi contro strutture sanitarie, supponendo che esse siano più disposte a pagare i riscatti richiesti per evitare ulteriori problemi. Una considerazione opposta invece è che le ransomware gang invece abbiano ridotto gli attacchi contro strutture sanitarie, per evitare di attirare su di sé eccessive attenzioni da parte delle autorità.

Gli attacchi selezionati sono quelli per cui è stato possibile trovare informazioni liberamente accessibili, e per i quali c'è stato un fermo documentato dei sistemi (o di una loro parte) o per i quali si è verificata una violazione dei personali. Questi attacchi e le difese adottate dalle strutture sanitarie possono fornire informazioni utili per delineare le contromisure più efficaci contro questo tipo di attacchi.

Per ogni attacco si cerca di ricostruire la sequenza dei principali avvenimenti, dalla scoperta dell'infezione dei sistemi fino al ripristino degli stessi,

avvenuto con il ripristino dei backup o pagamento del riscatto. La maggior parte degli attacchi segue una serie di passi, atti ad ottenere il controllo della rete informatica, caricare il malware sui dispositivi bersagliati e poi eseguirlo. Ripercorrendo questa catena di eventi è possibile comprendere i punti fondamentali dell'attacco, capire se le difese approntate hanno funzionato ed eventualmente idearne di nuove.

In particolare, sono analizzati i principali errori umani commessi che hanno facilitato l'attacco e come gli attaccanti abbiano sfruttato tali errori e i punti deboli della sicurezza della struttura sanitaria. Questo perché il principali punto debole dei sistemi informatici è chi li utilizza. Una persona potrebbe utilizzare impropriamente un sistema, magari aggirando le procedure di sicurezza implementate al fine di ottenere ciò che vuole più rapidamente.

Una volta compreso come avvengono questi attacchi, si procede a considerare l'impatto sulla protezione dei dati personali, soprattutto nei casi in cui si ha avuto furto dei dati presenti nei sistemi. Come scritto sopra, il tema della protezione di dati personali ha acquisito una notevole importanza a seguito dell'approvazione del GDPR.

Infine sono presentate delle possibili contromisure che permetto di gestire meglio il rischio collegato ad un attacco ransomware o wiper.

All'interno di questo documento non sono forniti dettagli tecnici esaustivi sul funzionamento dei malware utilizzati dagli attaccanti, solo i dettagli necessari su come sia stato effettuato l'attacco. L'obiettivo di questo documento è quello di illustrare i motivi per cui non si dovrebbe dimenticare il tema della sicurezza informatica in una struttura sanitaria.

4 Risultati

4.1 Wiper

Nel periodo selezionato non sono stati individuati attacchi che hanno utilizzato wiper contro strutture sanitarie. Sebbene in concomitanza dell'invasione russa dell'Ucraina siano emerse numerose varianti di wiper, esse sono utilizzate contro altri tipi di infrastruttura e servizi.

Un'ipotesi per spiegare questo fatto è che la maggior parte dei gruppi di cyber criminali sia interessata ad ottenere un guadagno economico dall'attacco, mentre attacchi con wiper sono fatti principalmente per causare un danno.

4.2 Diffusione degli attacchi ransomware

Le statistiche relative ad attacchi ransomware in generale mostrano che c'è stato un incremento negli anni 2020-2021 rispetto al 2019, riportandosi sui livelli del 2016. Nel dettaglio, il 2016 è finora l'anno con più attacchi ransomware registrati, pari a circa 638 milioni, seguito dal 2021, con circa 623 milioni di attacchi. Tra il 2017 e il 2019 c'è stato un notevole calo degli attacchi rispetto al 2016, con un numero di attacchi registrati pari a circa un terzo di quelli registrati nel 2016. Gli attacchi poi tornano a crescere nel 2020, attestandosi a circa 304 milioni di attacchi registrati. I dati parziali relativi al primo semestre del 2022 mostrano un numero di attacchi non troppo lontano da quelli del 2021, con 236 milioni di attacchi registrati finora [10].

Per quanto riguarda il settore sanitario, secondo un sondaggio condotto da Sophos nel 2021, il 34% delle organizzazioni sanitarie è stata colpita da un attacco ransomware nel 2020. Nel 65% dei casi gli attaccanti sono riusciti a cifrare i dati dati, ma solo nel 44% di questi casi i dati sono stati ripristinati tramite backup. Per i punti considerati, il settore sanitario fa peggio rispetto alla media di tutti i settori: nel 54% dei casi i cyber criminali sono riusciti a cifrare i dati e nel 39% dei casi l'attacco è stato fermato prima della cifratura, contro il 28% del settore sanitario [11]. Il sondaggio condotto da Sophos nel 2022 fornisce considerazioni simili, le quali evidenziano un aumento delle organizzazioni sanitarie colpite, 66% nel 2021 [12].

Durante il periodo pandemico alcune ransomware gangs hanno annunciato una sorta di "tregua" nei confronti delle strutture sanitarie impegnate nella risposta alla pandemia. Per esempio, il gruppo Maze ha annunciato, il 18 marzo 2020, che avrebbe fornito sconti per i riscatti da pagare, oltre a non colpire le strutture sanitarie fino a quando la situazione pandemica non si fosse stabilizzata. Altri gruppi come DoppelPaymer hanno ribadito la loro politica di non attacare strutture sanitarie o emergenziali, fornendo la possibilità di decifrare gratuitamente i dati in caso di un attacco per caso [13] [14] [15].

4.3 Analisi di alcuni attacchi

4.3.1 Attacco ransomware contro l'HSE

L'attacco ransomware più importante avvenuto in territorio europeo è quello contro il sistema sanitario irlandese (Health Service Executive, HSE). Il 14 maggio 2021 l'HSE è stato colpito da un attacco ransomware che ha portato

al fermo della maggior parte sistemi informatica in tutta la nazione. La compromissione iniziale dei sistemi risale al 18 marzo 2021, quando gli attaccanti sono riusciti ad ottenere il controllo di una workstation. Gli attaccanti hanno aspettato due mesi prima di iniziare l'attacco vero e proprio il 7 maggio. Il 21 maggio vengono ottenute le chiavi per la decifrazione e il 21 settembre si ha il completo ripristino dei sistemi.

Questo attacco ha comportato il ritorno a carta e penna per la maggior parte del personale dell'ospedale. L'80% dei sistemi informatica era stato compromesso dall'attacco ed era impossibile accedere alle cartelle mediche e le diagnosi dei pazienti che avevano ricevuto la vaccinazione anti-COVID. Oltre 700 GB di dati non cifrati, contenenti dati personali dei pazienti sono stati rubati dagli attaccanti [16].

Un medico intervistato da MalwareBytes, azienda operante nel settore della sicurezza informatica, ha fornito ulteriori dettagli sulle conseguenze dell'attacco. In particolare, per lo staff dell'ospedale era impossibile accedere alle email e l'utilizzo di carta e penna aveva reso molto difficile l'organizzazione del lavoro all'interno del suo ospedale [17].

A seguito dell'attacco sono state condotte della analisi per capire cosa non avesse funzionato. Il primo problema individuato è stato l'assenza di un singolo responsabile per la cybersecurity o, in generale, un dirigente che avesse delle responsabilità per la cybersecurity. Questo porta ad una mancanza di attenzione sul tema ad un alto livello decisionale. Infatti i team con responsabilità relative alla cybersecurity erano sotto-finanziati.

Sono poi presenti altri fattori da considerare. Un sistema antivirus è una delle possibili difese che si possono adottare, ma oggi da solo non basta. Il modello da seguire è quella della *difesa in profondità*, o a strati, in cui si utilizzano varie tecniche per difendere i propri sistemi. Per esempio il monitoraggio dei sistemi avrebbe aumentato le probabilità di individuare l'attacco in corso prima della cifratura dei dati, considerato che l'attaccante non aveva fatto tutto il possibile per nascondere le proprie tracce.

Infine c'è anche l'aspetto umano da considerare: il personale deve essere preparato ad affrontare una situazione di questo tipo. I membri dei team di cybersecurity devono essere in grado di eseguire le procedure di sicurezza decise. Per quanto riguarda gli altri dipendenti, è possibile insegnare loro come evitare email di phishing per esempio, riducendo in questo modo le probabilità di infezione dei sistemi. Per farlo si potrebbe inviare loro, più o meno spesso, delle email di test, per verificare il grado di attenzione.

4.3.2 Attacco contro la regione Lazio

Il 1 agosto 2021, la regione Lazio avvisa di un attacco in corso contro i suoi sistemi. A causa di ciò la piattaforma regionale per la prenotazione dei vaccini COVID diventa inaccessibile fino al 5 agosto. Nonostante questo attacco non sia propriamente contro una struttura sanitaria, esso è stato incluso per via del modo in cui è avvenuto.

Per spiegare questo attacco, l'ipotesi è che gli attaccanti abbiano avuto accesso ad un account di un dipendente LazioCrea (azienda della regione Lazio). Gli attaccanti hanno poi installato il ransomware nei sistemi, andando a cifrare i dati presenti su alcune macchine virtuali. La regione Lazio disponeva solo di backup online, i quali sono stati cancellati (ma non cifrati) dagli attaccanti. Grazie a ciò è stato possibile ripristinare i dati [18] [19].

Il fatto che a partire da un account di un dipendente sia stato possibile cifrare i dati di una buona parte del sistema è un problema. La gestione corretta dei privilegi utente è fondamentale per garantire la sicurezza dei sistemi. Inoltre è necessario considerare bene anche i propri fornitori, come si vede bene anche nel prossimo caso analizzato.

4.3.3 Il caso Blackbaud

Il 26 luglio 2020 Blackbaud, un provider di cloud computing, notifica ai propri clienti che, tra il 7 febbrario e il 20 marzo 2020, sono stati effettuati accessi non autorizzati ai propri dati. Tra i suoi clienti figurano anche organizzazioni sanitarie, le quali hanno notificato la violazione dei dati personali a milioni di individui. Questo ha portato ad alcune class-action contro Blackbaud [20] [21] [22].

Questo attacco evidenzia ulteriormente il rischio legato all'utilizzo di software di terze parti. Dal punto di vista della sicurezza è necessario che anche i fornitori di tali software rispettino standard di sicurezza stringenti, altrimenti gli sforzi della nostra organizzazione in tal senso saranno vanificati.

4.3.4 L'attacco contro lo Yuma Regional Medical Center

Lo Yuma Regional Medical Center in Arizona è un esempio di struttura sanitaria colpita da ransomware che, grazie a backup e procedure di emergenza, è riuscita a mantenere i sistemi operativi. L'attacco ransomware è stato individuato il 25 aprile 2022, attacco che ha colpito alcuni dei sistemi della struttura. Secondo le dichiarazioni dell'ospedale, sono state prese immediate

contromisure per limitare l'impatto dell'attacco e sono state messe in atto procedure di emergenza per garantire l'operatività dei sistemi.

Nonostante ciò. gli attaccanti sono riusciti a trafugare una parte dei dati presenti, prima di cifrarli. I dati personali (informazioni sull'assicurazione sanitaria, numero di previdenza sociale (SSN) e alcune informazioni mediche) di circa 700 000 individui sono stati esposti [23] [24].

4.4 Costo di un attacco ransomware

Il principale aspetto legato ad un attacco ransomware è il costo economico, non soltanto in termini di riscatto da pagare, ma anche in termini di downtime dei sistemi. Secondo un rapporto IBM sui costi di un data breach, il costo di un data breach in ambito sanitario è pari a circa 10.10 milioni di dollari, con il settore sanitario che per il dodicesimo anno di fila ha il costo medio maggiore di un data breach rispetto ad altri settori [25].

Questo costo non è dovuto tanto al pagamento del riscatto, quanto al costo necessario per ripristinare i sistemi. Infatti, sempre secondo il sondaggio condotto da Sophos nel 2022, il settore sanitario presentava il riscatto pagato più basso tra tutti quelli considerati, circa 197 mila dollari, nonostante considerando il volume complessivo fosse al primo posto. Questo perché la maggior parte delle organizzazioni sanitarie, soprattutto quelle pubbliche non ha a disposizione grandi quantità di denaro per pagare riscatti ingenti [12]. Il rapporto IBM riporta anche come non basta avere un incident response plan (IR) per ridurre i costi, ma serve anche verificare che tale piano funzioni. Chi ha verificato regolarmente che il piano funzioni correttamente ha riportato un risparmio di 2.66 milioni di dollari per data breach rispetto a chi non lo ha fatto.

Oltre a questi costi, bisogna considerare anche l'aspetto legale di questi attacchi. Il GDPR prescrive degli obblighi da rispettare in materia di protezione dei dati. L'art. 83 descrive tre possibili situazioni in cui si può incorrere in una sanzione amministrativa, a seconda del tipo di violazioni constatato. Viene dato un peso particolare alle violazioni riguardanti i principi di base del trattamento (articoli 5, 6, 7 e 9) e i diritti dei soggetti interessati dal trattamento (articoli da 12 a 22) tra le altre, con sanzioni che possono arrivare fino a 20 milioni di euro o il 4% del fatturato annuo. Nel caso di violazioni degli obblighi del titolare del trattamento (l'azienda sanitaria nel nostro caso) e del responsabile del trattamento si possono avere invece sanzioni amministrative fino a 10 milioni di euro o il 2% del fatturato annuo [26].

L'ammontare della sanzione è deciso tenendo in considerazione alcuni aspetti, descritti nel paragrafo 2 dell'articolo 83 e riportati qui sotto:

- la natura, la gravità e la durata della violazione
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati
- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi
- **le categorie di dati personali interessate dalla violazione**
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione
- rispetto dei provvedimenti presi da parte dell'autorità di controllo, nei confronti del titolare del trattamento o del responsabile del trattamento in questione, relativamente allo stesso oggetto
- l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso

È bene ricordare che tra i dati personali trattati dalle strutture sanitarie ci sono anche quelli relativi alla salute dell'individuo, i quali presentano delle restrizioni per quanto riguarda le finalità di trattamento. Per garantire il rispetto delle norme, e quindi evitare di incorrere in sanzioni in caso di attacco, è necessario prendere provvedimenti fin dalla fase di progettazione dei sistemi, al fine di garantire il rispetto di standard di sicurezza elevati.

5 Conclusione

In conclusione, gli attacchi che fanno utilizzo di wiper non sono ancora molto diffusi, sebbene ci sia stato un aumento soprattutto a causa dell'invasione russa dell'Ucraina.

Invece, per quanto riguarda gli attacchi ransomware contro strutture sanitarie, essi sono in aumento rispetto agli anni precedenti e c'è ancora un numero significativo di strutture che non hanno predisposto adeguate misure per gestire il rischio.

Questo rischio va gestito implementando adeguate piani di risposta per incidenti informatici. Sono necessarie procedure per ripristinare i sistemi, utilizzando per esempio backup, ma anche procedure per gestire eventuali data breach.

Altre misure da predisporre sono l'introduzione di sistemi di monitoraggio dei sistemi adeguati e un adeguato investimento in una squadra che si occupa di cybersecurity. Preparare il personale ad affrontare situazioni di emergenza è altrettanto importante.

Riferimenti bibliografici

[1] «Ransomware,» *NIST*, 27 set. 2021, Last Modified: 2022-09-14T16:01-04:00. indirizzo: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware (visitato il 13/11/2022).

[2] «What is double extortion ransomware?» Zscaler. (13 nov. 2022), indirizzo: https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware (visitato il 13/11/2022).

[3] «Ransomware gang,» Ransomware.org. (13 nov. 2022), indirizzo: https://ransomware.org/glossary-of-terms/ransomware-gang/ (visitato il 13/11/2022).

[4] «Ransomware as a Service (RaaS) - Definition.» (13 nov. 2022), indirizzo: https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas (visitato il 13/11/2022).

[5] «What is ransomware as a service (RaaS)? the dangerous threat to world security — UpGuard.» (13 nov. 2022), indirizzo: https://www.upguard.com/blog/what-is-ransomware-as-a-service (visitato il 13/11/2022).

[6] *Wiper (malware)*, in *Wikipedia*, Page Version ID: 1113311422, 30 set. 2022. indirizzo: https://en.wikipedia.org/w/index.php?title=Wiper_(malware)&oldid=1113311422 (visitato il 13/11/2022).

[7] G. Revay. «An overview of the increasing wiper malware threat — FortiGuard labs,» Fortinet Blog. Section: Threat Research. (28 apr. 2022), indirizzo: https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat (visitato il 13/11/2022).

[8] *Regolamento generale sulla protezione dei dati*, in *Wikipedia*, Page Version ID: 130370140, 8 nov. 2022. indirizzo: https://it.wikipedia.org/w/index.php?title=Regolamento_generale_sulla_protezione_dei_dati&oldid=130370140 (visitato il 23/11/2022).

[9] «Data Breach - Violazioni di dati personali.» (13 nov. 2022), indirizzo: https://www.garanteprivacy.it/data-breach (visitato il 13/11/2022).

[10] «Number of ransomware attacks per year 2022,» Statista. (23 nov. 2022), indirizzo: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (visitato il 23/11/2022).

[11] «Sophos — The State of Ransomware in Healthcare 2021.» (23 nov. 2022), indirizzo: https://assets.sophos.com/X24WTUEQ/at/s49k3zrbsj8x9hwbm9nkhzxh/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf (visitato il 23/11/2022).

[12] «Sophos — The State of Ransomware in Healthcare 2022.» (23 nov. 2022), indirizzo: https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf (visitato il 23/11/2022).

[13] «Ransomware groups say they won't attack hospitals.» (13 nov. 2022), indirizzo: https://www.virsec.com/blog/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word (visitato il 13/11/2022).

[14] «The top 5 cyber threats in the healthcare industry.» (13 nov. 2022), indirizzo: https://www.avertium.com/resources/threat-reports/cyber-threats-in-the-healthcare-industry (visitato il 13/11/2022).

[15] «Lockbit 2.0 ransomware: An in-depth look at lockfile & LockBit.» (23 nov. 2022), indirizzo: https://www.avertium.com/blog/lockbit-2.0-ransomware-lockfile (visitato il 23/11/2022).

[16] S. Attaway. «Case study: Ransomware locks up 80% of 54-hospital health system,» Meditology Services. (14 feb. 2022), indirizzo: https://www.meditologyservices.com/case-study-ransomware-locks-up-80-of-54-hospital-health-system/ (visitato il 13/11/2022).

[17] «A doctor reveals the human cost of the HSE ransomware attack,» Malwarebytes. (13 nov. 2022), indirizzo: https://www.malwarebytes.com/blog/news/2021/05/a-doctor-reveals-the-human-cost-of-the-hse-ransomware-attack (visitato il 13/11/2022).

[18] «Regione Lazio e ransomware, lieto fine amaro: troppi errori fatti,» Cyber Security 360. (8 ago. 2021), indirizzo: https://www.cybersecurity360.it/nuove-minacce/regione-lazio-vaccini-bloccati-poco-pronta-contro-il-ranwomare-ecco-perche/ (visitato il 22/11/2022).

[19] «Ransomware attack hits italy's lazio region, affects COVID-19 site,» BleepingComputer. (22 nov. 2022), indirizzo: https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/ (visitato il 22/11/2022).

[20] «Recent Spike in Healthcare Breach Reports Due To Blackbaud Ransomware Attack — Critical Insight.» (13 nov. 2022), indirizzo: https://www.criticalinsight.com/resources/news/article/recent-spike-in-healthcare-breach-reports-due-to-blackbaud-ransomware-attack (visitato il 13/11/2022).

[21] «Blackbaud hack: US healthcare organizations confirm data breach impacted 190,000 patients,» The Daily Swig — Cybersecurity news and views. (16 set. 2020), indirizzo: https://portswigger.net/daily-swig/blackbaud-hack-us-healthcare-organizations-confirm-data-breach-impacted-190-000-patients (visitato il 13/11/2022).

[22] HealthITSecurity. «Blackbaud faces another lawsuit, as more healthcare victims reported,» HealthITSecurity. (24 nov. 2020), indirizzo: https://healthitsecurity.com/news/blackbaud-faces-another-lawsuit-as-more-healthcare-victims-reported (visitato il 13/11/2022).

[23] H. Journal. «700,000 patients affected by yuma regional medical center ransomware attack,» HIPAA Journal. (13 giu. 2022), indirizzo: https://www.hipaajournal.com/700000-patients-affected-by-yuma-regional-medical-center-ransomware-attack/ (visitato il 13/11/2022).

[24] «Healthcare breaches on the rise in 2022,» SearchSecurity. (13 nov. 2022), indirizzo: https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise (visitato il 13/11/2022).

[25] «Cost of a data breach 2022.» (7 nov. 2022), indirizzo: https://www.ibm.com/reports/data-breach (visitato il 13/11/2022).

[26] «Regolamento GDPR.» (), indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT#d1e3043-1-1 (visitato il 17/12/2022).