Report

Approfondimento sulla strutturazione e la difesa di attacchi ransomware.

Emanuela Elli - 892901

CdLM Data Science

Università degli studi di Milano Bicocca

Corso di Cybersecurity

Anno Accademico 2022-2023

1. Introduzione

La moderna tendenza di attacchi ransomware è iniziata con l'epidemia di WannaCry del 2017. WannaCry è un worm, di tipologia ransomware, responsabile di aver infettato i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo su computer con Microsoft Windows nel maggio 2017, incluso anche alcuni computer dell'università Bicocca. In esecuzione cripta i file presenti sul computer e chiede un riscatto di alcune centinaia di dollari per decriptarli. Questo attacco su larga scala ha dimostrato che gli attacchi ransomware erano possibili e potenzialmente redditizi. Da allora, decine di varianti di ransomware sono state sviluppate e utilizzate in una varietà di attacchi.

Anche la pandemia di COVID-19 ha contribuito alla recente ondata di ransomware. Man mano che le organizzazioni passavano rapidamente al lavoro da remoto, si creavano lacune nelle loro difese informatiche. I criminali informatici hanno sfruttato queste vulnerabilità per distribuire ransomware provocando un'ondata di attacchi.

Il ransomware è un software che può crittografare tutti i tuoi dati o impedire l'utilizzo del computer. Una volta che il ransomware è stato installato sul computer, richiederà un riscatto, spesso in criptovaluta, in cambio della mancata divulgazione o della vendita delle informazioni e al fine di decrittografare i dati o sbloccare il computer.

2. Strutturazione dell'attacco

In un attacco ransomware, gli hacker utilizzano malware per crittografare, eliminare o manipolare dati, la proprietà intellettuale o le informazioni personali. Ciò consente agli aggressori di tenere in ostaggio digitale le informazioni, il dispositivo o il sistema fino a quando la vittima non soddisfa le richieste di riscatto del criminale informatico, che di solito comportano un pagamento sicuro e non rintracciabile. Il ransomware rimane una delle tattiche più redditizie per i criminali informatici, con crescenti richieste di riscatto che spesso vanno da 1 milione di dollari a 10 milioni di dollari. È importante notare che il pagamento della richiesta di riscatto dell'hacker non garantisce che il sistema verrà ripristinato o che i dati rubati non verranno condivisi o venduti sul dark web.

Esistono molti tipi di ransomware e, con le nuove minacce ransomware che si sviluppano regolarmente, potrebbe essere difficile rintracciarle tutte. Queste sono le famiglie di ransomware segnalate più spesso, secondo le informazioni della società di sicurezza informatica Coveware:

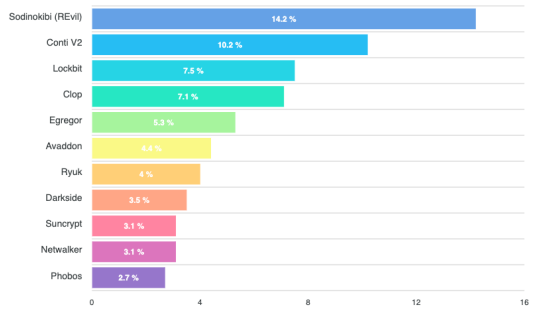

Figura 1. Percentuale dei primi 10 tipi di ransomware segnalati (Fonte: Cloudwards.net)

Per avere successo, il ransomware deve ottenere l'accesso a un sistema di destinazione, crittografare i file presenti e richiedere un riscatto alla vittima. Inoltre anche se i dettagli di implementazione variano da una variante di ransomware all'altra, tutti condividono le stesse tre fasi fondamentali mostrate di seguito.

2.1. Passaggio 1: Attacco e vettori di distribuzione

Il ransomware, come qualsiasi malware, può accedere ai sistemi di un'organizzazione in diversi modi. Tuttavia, gli operatori di ransomware tendono a preferire alcuni vettori di infezione specifici. Uno di questi è l'e-mail di phishing, ovvero un'e-mail dannosa che può contenere un collegamento a un sito Web che ospita un download dannoso oppure un allegato con funzionalità di downloader integrate. In questo modo il ransomware viene scaricato ed eseguito sul proprio computer, qualora l'utente si facesse ingannare.
Un altro popolare vettore di infezione da ransomware sfrutta servizi come il Remote Desktop Protocol (RDP). Con questo protocollo un utente malintenzionato, che ha rubato o indovinato le credenziali di accesso di un dipendente, può autenticarsi ed accedere in remoto ad un computer della rete aziendale. Tramite questo accesso, l'attaccante può scaricare direttamente il malware ed eseguirlo sulla macchina sotto il suo contro-

llo.
Altri potrebbero tentare di infettare direttamente i sistemi, come il worm WannaCry ha sfruttato la vulnerabilità EternalBlue (nome di un exploit che si ritiene sia stato scritto dalla National Security Agency).
In realtà bisogna considerare che la maggior parte delle varianti di ransomware ha più vettori di infezione.

2.2. Passaggio 2: Crittografia

Dopo che si è ottenuto l'accesso ad un sistema, è possibile iniziare a crittografare i file. Poiché la funzionalità di crittografia è integrata in un sistema operativo, questo implica semplicemente l'accesso ai file, la loro crittografia con una chiave controllata da un utente malintenzionato e la sostituzione degli originali con le versioni crittografate.
La maggior parte delle varianti di ransomware è cauta nella selezione dei file da crittografare per garantire la stabilità del sistema. Alcune varianti adottano anche misure per eliminare il backup e le copie shadow dei file (copie di backup del contenuto di file, cartelle e interi volumi creati in un dato istante) per rendere più difficile il ripristino senza la chiave di decrittazione.

2.3. Passaggio 3: Riscatto

Una volta completata la crittografia dei file, il ransomware è pronto a presentare una richiesta di riscatto. Diverse varianti di ransomware lo implementano in numerosi modi, ma non è raro che lo sfondo del display venga modificato in una nota di riscatto o in file di testo inseriti in ciascuna directory crittografata contenente la richiesta di riscatto. In genere, viene richiesta una determinata quantità di criptovaluta in cambio dell'accesso ai file della vittima.
Se il riscatto viene pagato, l'operatore del ransomware fornirà una copia della chiave privata utilizzata per proteggere la chiave di crittografia simmetrica o una copia della chiave di crittografia simmetrica stessa. Queste informazioni possono essere inserite in un programma di decrittazione (anch'esso fornito dal criminale informatico) che può utilizzarle per invertire la crittografia e ripristinare l'accesso ai file dell'utente.

Sebbene questi tre passaggi fondamentali esistano in tutte le varianti di ransomware, diversi ransomware possono includere implementazioni diverse o passaggi aggiuntivi. Ad esempio, varianti di ransomware come Maze eseguono la scansione di file (o anche informazioni di registro) ed eseguono il furto di dati prima della crittografia dei dati, mentre il ransomware WannaCry esegue la scansione di altri dispositivi vulnerabili da infettare e crittografare.

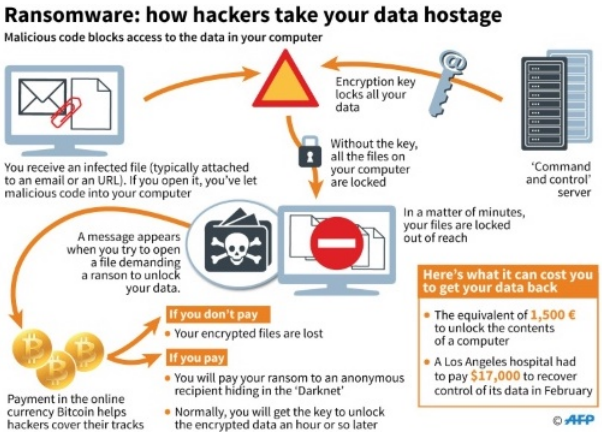

Figura 2. Immagine esplicativa di come viene attuato un attacco ransomware (Fonte: EagleNews).

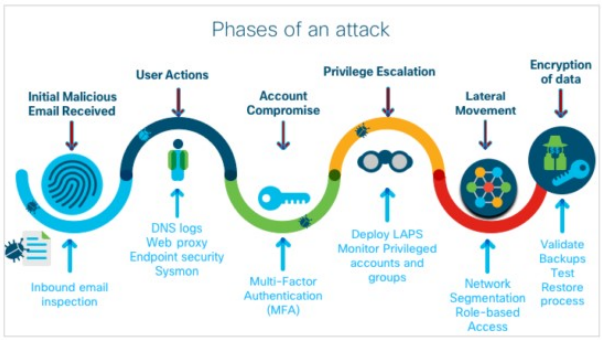

Figura 3. Fasi di un attacco ransomware (Fonte: Ciscocrep). Il Lateral movement consente agli hacker di entrare più in profondità in un sistema per tenere traccia di dati sensibili e altre risorse di alto valore. L'autore della minaccia ottiene inizialmente l'accesso al sistema tramite un endpoint tramite un attacco di phishing o ransomware o un'infezione da malware.

3. Come affrontarlo

Una preparazione adeguata può ridurre drasticamente il costo e l'impatto di un attacco ransomware. L'adozione delle seguenti best practice può ridurre l'esposizione di un'organizzazione al ransomware e minimizzarne l'impatto:

1. **Formazione e istruzione sulla consapevolezza informatica:** il ransomware viene

spesso diffuso tramite e-mail di phishing. La formazione degli utenti su come identificare ed evitare potenziali attacchi ransomware è fondamentale. Poiché molti degli attuali attacchi informatici iniziano con un'e-mail mirata che non contiene nemmeno malware, ma solo un messaggio di social engeneering che incoraggia l'utente a fare clic su un collegamento dannoso. L'educazione dell'utente è spesso considerata una delle difese più importanti un'organizzazione può distribuire.

2. **Backup continui dei dati:** la definizione di ransomware dice che si tratta di malware progettato in modo che l'unico modo per ripristinare l'accesso ai dati crittografati sia il pagamento di un riscatto. I backup dei dati automatizzati e protetti consentono a un'organizzazione di riprendersi da un attacco con una perdita di dati minima e senza pagare un riscatto. Il mantenimento di backup regolari dei dati come processo di routine è una pratica molto importante per prevenire la perdita di dati e per poterli recuperare in caso di danneggiamento o malfunzionamento dell'hardware del disco.
3. **Applicazione di patch:** è fondamentale poiché i criminali informatici spesso cercano gli ultimi exploit scoperti nelle patch (serie di comandi progettati per aggiornare o risolvere un problema o una vulnerabilità del software) rese disponibili, per cui prendono di mira i sistemi che non sono ancora stati patchati. Pertanto, è fondamentale che le organizzazioni assicurino che a tutti i sistemi siano applicate le patch più recenti, in quanto riduce il numero di potenziali vulnerabilità all'interno dell'azienda che un utente malintenzionato può sfruttare.
4. **Autenticazione utente:** l'accesso a servizi come RDP (Remote Desktop Protocol) con credenziali utente rubate è una delle tecniche preferite dagli aggressori ransomware. L'uso dell'autenticazione utente avanzata può rendere più difficile per un utente malintenzionato utilizzare una password indovinata o rubata.

3.1. Come rimuovere il ransomware?

È possibile adottare alcune misure per rispondere ad un attacco di ransomware e scegliere se pagare o meno il riscatto. Molti attacchi ransomware riusciti vengono rilevati solo dopo che la crittografia dei dati è stata completata e una richiesta di riscatto è stata visualizzata sullo schermo del computer infetto ma, in tal modo, i file crittografati sono con buona probabilità irrecuperabili. Perciò in caso di attacco è necessario eseguire immediatamente alcune buone pratiche per aumentare la probabilità di recupero dei dati:

1. Mettere in quarantena la macchina, ovvero limitare la diffusione del malware rimuovendo l'accesso ad altri potenziali bersagli.
2. Tenere il computer acceso per massimizzare la probabilità di recupero (lo spegnimento di un computer può causare la perdita di memoria volatile).
3. Creare una copia dei file (backup) crittografati su un supporto rimovibile, nel caso in cui una soluzione diventi disponibile in futuro o un tentativo di decrittazione fallito danneggi i file.
4. Controllare con No More Ransom Project (iniziativa intrapresa dal National High Tech Crime Unit della polizia olandese, dall' European Cybercrime Centre dell'Europol ed altri enti, con l'obiettivo di aiutare le vittime del ransomware a recuperare i loro dati criptati, senza dover pagare i criminali) per vedere se è disponibile un decryptor gratuito. In tal caso, eseguirlo su una copia dei dati crittografati per vedere se è possibile ripristinare i file.
5. Affidarsi ad un esperto di digital forensics che potrebbe essere in grado di recuperare le copie di backup dei file archiviati se non sono state eliminate dal malware.
6. Ripristinare la macchina da un backup pulito o dall'installazione del sistema operativo. Ciò garantisce che il malware venga completamente rimosso dal dispositivo.

4. Settori più colpiti

Tramite lo studio Ransomware Intelligence Global Report 2023 svolto dall'azienda Coinnect, start-up che sviluppa soluzioni di cyber insurtech, si è dimostrato che nel corso del 2021 e del 2022 a livello globale gli attacchi ransomware sono diventati sempre più frequenti e sofisticati, rappresentando quindi uno dei principali problemi per le organizzazioni di tutte le dimensioni.

L'analisi dimostra che le piccole e medie imprese risultano le più bersagliate: sia nel 2021 che nel 2022 la maggior parte degli attacchi ha colpito organizzazioni con meno di 1.000 dipendenti e circa il 60 % delle aziende prese di mira

nel 2021 e nel 2022 ha meno di 250 dipendenti. A livello di aree geografiche, il Nord America si conferma al primo posto a livello mondiale per numero di attacchi, sebbene sia anche l'area che ha registrato il maggiore calo tra il 2021 ed il 2022 (-10 %). Segue l'Europa con il 26,73 % degli attacchi nel 2021 ed il 29,73 % nel 2022 e l'Asia con il 9,82 % nel 2021 ed il 15,41 % nel 2022.

Per quanto riguarda i settori, il più colpito nel 2021 è stato quello dei Beni di Consumo con il 28,1 % degli attacchi, seguito da quello dei Beni industriali con il 25,08 % e da quello Health con il 7,4 %; per quanto riguarda il 2022, invece, il settore più colpito è stato quello dei Beni Industriali con il 32 % degli attacchi, seguito dai Beni di Consumo con il 24,9 % e dal settore IT con il 10,6 %.

Il ransomware rappresenta oggi la principale causa dei sinistri assicurativi informatici e si prevede che questa tendenza continuerà anche in futuro. Uno dei motivi principali è che gli attacchi ransomware stanno diventando sempre più sofisticati: gli aggressori utilizzano tecniche sempre più avanzate per eludere il rilevamento e criptare i dati aziendali e ciò rende sempre più difficile per le organizzazioni prevenire e riprendersi dagli attacchi, aumentando le probabilità di successo della richiesta di riscatto. Un altro motivo è che molte piccole e medie imprese sono particolarmente vulnerabili agli attacchi ransomware, non disponendo delle risorse e delle competenze necessarie per proteggersi efficacemente. Questo le rende un obiettivo interessante per gli aggressori, che sanno che queste aziende sono più propense a pagare il riscatto per riottenere l'accesso ai propri dati.

Di seguito una previsione di quale sarà il costo totale dei danni da ransomware in tutto il mondo nel 2031:

Figura 4. Previsione costo totale dovuto ad attacchi ransomware (Fonte: Cloudwards.net).

5. Conclusioni

A conclusione di questo lavoro è possibile affermare che il ransomware è attualmente una minaccia globale sia per le organizzazioni che per gli individui. Dagli studi esposti, è possibile constatare che lo sviluppo tecnologico permetterà agli attaccanti di modellare tali worm in maniera sempre più specifica e veloce rispetto a quelli che saranno gli strumenti di difesa a disposizione, è necessario prender coscienza di quali siano le best practice da attuare affinchè il rischio venga ridotto al minimo possibile.
Delle buone norme includono necessariamente la formazione degli individui, l'aggiornamento continuo di sistemi operativi e software oltre che al monitoraggio del proprio ambiente e, quando possibile, l'investimento di tempo e denaro in tecniche di cybersecurity volte allo studio (ad esempio tramite sistemi honeypot) e allo sviluppo di nuove funzionalità o nuovi sistemi di sicurezza in grado di difendere maggiormente la vittima.

Sitografia

[1] Ransomware Attack – What is it and How Does it Work? Checkpoint.com

[2] Top Critical Vulnerabilities Used by Ransomware Groups, Socradar.io

[3] Ransomware Intelligence Global Report 2023: nell'ultimo biennio gli attacchi ransomware sono diventati sempre più frequenti e sofisticati, Assinews.it

[4] Ransomware Statistics, Trends and Facts for 2023 and Beyond, Cloudwards.net

[5] Cosa consente il ransomware agli hacker? Crowdstrike.com