Ransomware

Caratteristiche, preparazione e risposta agli attacchi ransomware

TLP:CLEAR

*Il presente documento ha un livello di condivisione **TLP:CLEAR.** Le informazioni possono essere distribuite senza restrizioni rispettando eventuali disposizioni sul copyright. Ulteriori dettagli sono disponibili sulla pagina dedicata del CSIRT Italia e sulla pagina dedicata del FIRST.*

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, anche attuando il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza, promuovendone azioni comuni.

L'Agenzia è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. In tale veste ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico del Paese promuovendo la realizzazione di azioni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese. A tal fine sviluppa anche capacità necessarie per proteggere dalle minacce informatiche reti, sistemi informativi e servizi informatici delle Pubbliche Amministrazioni e degli operatori di infrastrutture critiche nazionali, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Siti web: **Agenzia per la Cybersicurezza Nazionale** **CSIRT Italia**

Contatti: **info@acn.gov.it**

Seguici sui nostri canali social:

Esclusione di responsabilità

Il presente documento fornisce, a titolo esemplificativo e non esaustivo, indicazioni di mero ausilio alle attività di sicurezza dell'Organizzazione e non solleva la stessa dall'onere di porre in essere, nel rispetto della normativa vigente in materia di cybersicurezza, tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dal verificarsi di eventi e incidenti informatici.

SOMMARIO

EXECUTIVE SUMMARY

Il **ransomware** è una tipologia di minaccia che ha lo scopo di **cifrare i dati del bene informatico target** in modo da comprometterne la disponibilità, integrità e riservatezza. L'impatto di questi attacchi può essere di tipo **economico, operativo, reputazionale e legale.**

1989 — **AIDS Trojan**: primo esempio di attacco ransomware

2000 — **Diffusione di Internet**: aumento dei dispositivi connessi

2008 — **Nascita di criptovalute**: come Bitcoin

2017 — **Campagne ransomware di massa**: come Wannacry e NotPetya

2019 — **RaaS**: Diffusione modello Ransomware-as-a-Service

Kill chain del ransomware

Threat Actor e motivazioni

L'evoluzione della minaccia ransomware ha comportato una **riorganizzazione dell'ecosistema criminale**, sostenuto dalla **progressiva specializzazione** degli attaccanti e da una loro ristrutturazione in **ransomware gang**.

La specializzazione degli attaccanti ha permesso il raggiungimento di un grado di efficienza tale che alcuni gruppi hanno iniziato a offrire la propria infrastruttura anche ad utenti esterni al gruppo, spesso in cambio di una percentuale sul riscatto eventualmente ottenuto, un modello che prende il nome di **Ransomware-as-a-Service** e che permette **l'incremento dei profitti** degli attaccanti.

Difatti, le motivazioni di un attacco ransomware sono spesso di **tipo economico**. Le vittime vengono identificate in maniera opportunistica poiché possiedono caratteristiche che le rendono attaccabili.

Raccomandazioni e contromisure

Proteggere i propri asset dalla minaccia ransomware richiede **l'adozione di misure preventive**. Le raccomandazioni e le contromisure qui proposte sono articolate in tre tipologie.

Processi e strategie

Raccomandazioni relative alla preparazione e aggiornamento di **politiche organizzative**, piani di risposta e strategie di *recovery* e gestione del rischio.

Soluzioni di sicurezza

Raccomandazioni relative alle **soluzioni tecnologiche** da adottare per migliorare la capacità di tracciamento, monitoraggio e gestione di un incidente.

Controlli di sicurezza

Raccomandazioni relative alle **misure di sicurezza** e ai **processi tecnici** quali l'adozione di MFA, il controllo degli accessi e la cifratura dei dati sensibili.

1 RANSOMWARE LANDSCAPE

Il presente capitolo offre un'introduzione alla minaccia ransomware, fornendone una **definizione** e illustrando le **principali evoluzioni** del modello criminale avvenute nel corso degli ultimi anni. Il capitolo si conclude con **un'analisi della minaccia in Italia,** offrendo una sintetica evidenza della sua distribuzione temporale e geografica, oltre che dei settori colpiti più frequentemente.

Le definizioni incluse in questo documento sono in linea con quelle presenti nella Tassonomia Cyber dell'ACN. In caso di necessità, la Guida alla notifica degli incidenti al CSIRT Italia fornisce indicazioni relative alle modalità di notifica predisposte.

1.1 Definizione

Il ransomware è una tipologia di minaccia che ha lo scopo di **cifrare i dati del bene informatico target** in modo da comprometterne la disponibilità, integrità e riservatezza. Inoltre, in questa tipologia di minaccia spesso l'attaccante crea dei file, detti *ransom notes*, tramite i quali viene richiesto alla vittima un **riscatto in cambio dell'accesso ai propri dati**. In alcuni casi i dati, prima di essere cifrati, vengono esfiltrati in modo da offrire all'attaccante uno strumento in più di ricatto nei confronti della vittima.

A seconda del loro funzionamento, i ransomware possono dividersi in **automatizzati** o ***human-operated***. Nel caso dei ransomware automatizzati, l'attacco si diffonde come un virus in **modo autonomo**, spesso ricorrendo ad e-mail di phishing come vettore d'attacco. Gli *human-operated* ransomware sono invece il risultato di un'azione condotta direttamente da un attaccante, spesso a seguito del furto di credenziali. Rispetto ai ransomware automatizzati, gli *human-operated* permettono agli attaccanti di pianificare meglio gli attacchi, selezionare i propri target e massimizzare gli impatti, rispondendo più velocemente alle evoluzioni della minaccia cyber nell'ultimo decennio.

Sulla base della loro modalità di azione, invece, si definiscono ***crypto ransomware* o *encryptors*** quei ransomware che utilizzano la crittografia per rendere indisponibili i dati in un sistema, ***lockers*** quelli che rendono inaccessibili i sistemi richiedendo il pagamento del riscatto, e ***scareware*** quelli che inducono le vittime a scaricare o acquistare un software malevolo per risolvere una criticità

artefatta e appositamente creata dall'attore criminale[1]. Si definiscono inoltre ***doxware*** e ***leakware*** quelle tipologie di ransomware che minacciano la pubblicazione dei dati sensibili della vittima. A queste categorie si aggiunge il ***Ransomware-as-a-Service*** **(RaaS)**, ovvero una tipologia di attacco condotto da operatori specializzati di cui si darà maggiore contesto nella sezione successiva.

A prescindere dalla natura e dalla capacità di azione di un ransomware, le sue conseguenze sulle vittime possono essere molteplici. In primo luogo, **l'impatto degli attacchi può essere di tipo economico**, considerando il costo del riscatto eventualmente pagato, i danni economici derivanti dall'interruzione o rallentamento delle operazioni e i costi di ripristino dei sistemi e delle informazioni.

In secondo luogo, gli **impatti possono essere operativi** qualora si verifichi una perdita di dati a seguito della loro cifratura o non si disponga di backup aggiornati. Tali effetti possono essere ancora più rilevanti qualora gli attaccanti conducano parallelamente attacchi DDoS contro le vittime, una pratica adottata da alcuni attori criminali per esercitare una maggiore pressione sulle vittime e indurle a pagare il riscatto.

Il **danno reputazionale** è un'ulteriore tipologia di impatto frequentemente sperimentato dalle vittime di ransomware, in quanto le organizzazioni colpite sono spesso percepite pubblicamente come responsabili dell'inefficace gestione della sicurezza di dati e informazioni. A ciò si aggiunge infine l'esposizione a **rischi di natura legale** nel caso in cui i dati esfiltrati siano resi pubblici ma coperti dalle normative vigenti in materia di protezione dei dati personali.

1.2 Evoluzione della minaccia

Il primo esempio di attacco ransomware viene fatto risalire al 1989, quando 20.000 floppy disks contenenti il malware "PC Cyborg" vennero distribuiti ai partecipanti della conferenza organizzata dall'Organizzazione Mondiale della Sanità sull'AIDS, cifrando le informazioni presenti sui sistemi vittima e richiedendo il pagamento di un riscatto. Per questo motivo, l'attacco è noto come "AIDS Trojan"[2].

La **nascita di criptovalute,** come Bitcoin nel 2008 e Monero nel 2014, ha introdotto un'infrastruttura finanziaria che garantiva agli attaccanti maggiore segretezza e costi di transizione significativamente più bassi[3].

Tra gli altri fattori abilitanti, lo sviluppo delle criptovalute ha permesso la crescita del fenomeno e

[1] 5 Most Common Types of Ransomware - CrowdStrike, 2023

[2] Analyzing the History of Ransomware Across Industries - Fortinet, 2021

[3] Cyber threat bulletin: The ransomware threat in 2021 - Canadian Centre for Cyber Security, 2021; Analyzing the History of Ransomware Across Industries – Fortinet, 2021

lo sviluppo di **campagne ransomware di massa** quali Wannacry, responsabile nel 2017 dell'infezione di oltre 200.000 computer in 150 paesi, e NotPetya, responsabile nello stesso anno dell'attacco contro oltre 2.000 organizzazioni, di cui la maggior parte in Ucraina[4].

A partire dal 2019 il modello criminale dei ransomware si è trasformato, evolvendosi dall'**invio di allegati malevoli** indirizzati ad un ampio e generico spettro di potenziali target, con richieste estorsive spesso di entità contenuta, all'ascesa del modello di ***Ransomware-as-a-Service*** (RaaS).

Il RaaS determina una **compartimentazione dell'ecosistema criminale** del ransomware, in cui le varie componenti operative (dallo sviluppo del malware alla sua propagazione, dalla gestione delle infrastrutture di pagamento, di comando e controllo "C2" fino al processo di negoziazione) vengono delegate, dietro compenso, ad attori criminali con elevate competenze specialistiche[5]. Questo 'modello di business' criminale favorisce **una continua evoluzione del ransomware**, sostenuta da aggiornamenti sistematici degli sviluppatori, dall'ottimizzazione delle economie di scala e da una maggiore accessibilità del ransomware per un più ampio spettro di attori malevoli.

Contestualmente, gli attori criminali hanno perfezionato le metodologie di raccolta informativa e profilazione delle organizzazioni target. Queste attività, denominate "***Big Game Hunting***" (BGH), consentono alle 'ransomware gang' di selezionare gli obiettivi in base al loro potenziale economico e alla loro presumibile capacità di corrispondere riscatti significativi[6], calibrando così le richieste estorsive in funzione della solidità finanziaria dell'obiettivo[7].

Secondo il "Incident Response Report 2024"[8] di Palo Alto Networks, nel 2023 il **valore stimato dei riscatti richiesti** è aumentato di circa il 7% rispetto al 2022 (Figura 1), mentre nel 2023 il valore del **riscatto effettivamente pagato** equivale in termini di valore mediano a circa il 34% del valore originariamente richiesto nello stesso anno da parte degli attori criminali.

[4] Modern Ransomware and Its Evolution – Canadian Centre for Cyber Security, 2020
[5] Threat Landscape for Ransomware Attacks – ENISA, 2022
[6] RANSOMWARE - Evoluzione e misure di protezione - CSIRT Italia, 2021
[7] Threat Landscape for Ransomware Attacks – ENISA, 2022
[8] Incident Response Report – Palo Alto Networks, 2024

Anno	Riscatto richiesto (valore mediano)	Riscatto pagato (valore mediano)
2022	$ 650.000	$ 350.000
2023	$ 695.000	$ 237.500

Figura 1: Valore mediano dei riscatti richiesti e pagati nel 2022 e 2023 secondo il "Incident Response Report 2024" di Palo Alto Networks

Stimare la percentuale di vittime che concordano il pagamento del *ransom* è difficile. Ciononostante, secondo l'analisi condotta da ENISA e contenuta nel report "Threat Landscape for Ransomware Attacks"[9] pubblicato nel 2022, circa **il 62% delle vittime avrebbe negoziato con gli attaccanti per la corresponsione del riscatto**.

A partire dal 2019, in concomitanza con il perfezionamento delle tecniche di 'target selection', i gruppi specializzati hanno implementato strategie di esfiltrazione dei dati prima di avviarne la cifratura[10]. In tal modo, gli attori criminali possono minacciare le vittime di **divulgare le informazioni sottratte in caso di mancato pagamento del riscatto** o esigere pagamenti supplementari per prevenirne la pubblicazione su piattaforme dedicate denominate "*leak sites*". Questo modello operativo prende il nome di ***Double Extortion***, ed è mirato ad aumentare ulteriormente i profitti dei gruppi criminali[11].

Ad oggi, i proventi delle operazioni ransomware mostrano un trend di crescita costante, segnando nuovi record[12] e sottolineando l'urgenza di implementare contromisure mirate per il contenimento di questa minaccia.

1.3 Contesto nazionale

Negli ultimi anni il ransomware si è affermato come una delle **minacce prevalenti** a livello nazionale. Nonostante sia difficile stimarne il numero esatto, spesso per le mancate segnalazioni da parte delle vittime, il numero di ransomware seguiti dal CSIRT Italia è in **costante ascesa**. L'Italia si colloca, difatti, tendenzialmente al quarto posto fra le **nazioni europee maggiormente colpite** dalla minaccia ransomware (con il 12% dei casi in Europa), preceduta spesso da Gran

[9] Threat Landscape for Ransomware Attacks – ENISA, 2022
[10] RANSOMWARE - Evoluzione e misure di protezione - CSIRT Italia, 2021
[11] #StopRansomware Guide - Cybersecurity and Infrastructure Security Agency (CISA), 2023
[12] Ransomware Hit $1 Billion in 2023 – Chainalysis, 2024

Bretagna, Germania e Francia.

Come mostrato in Figura 2, le vittime appartengono prevalentemente al **settore privato,** con le **piccole imprese** che, spesso per una limitata attitudine ad una cultura della sicurezza, risultano essere la tipologia di target principale degli attaccanti. Analizzando la loro distribuzione in base ai settori di attività economica di appartenenza, il **manifatturiero** emerge come il settore maggiormente colpito, seguito da **altre** tipologie di **società private**, dal comparto della **vendita al dettaglio** e dall'industria **tecnologica**.

Da un punto di vista geografico, le zone più interessate dal fenomeno risultano essere **i grandi distretti industriali del Nord Italia,** ciò è presumibilmente determinato dalla maggiore presenza, in tali zone, di imprese operanti nel settore manifatturiero.

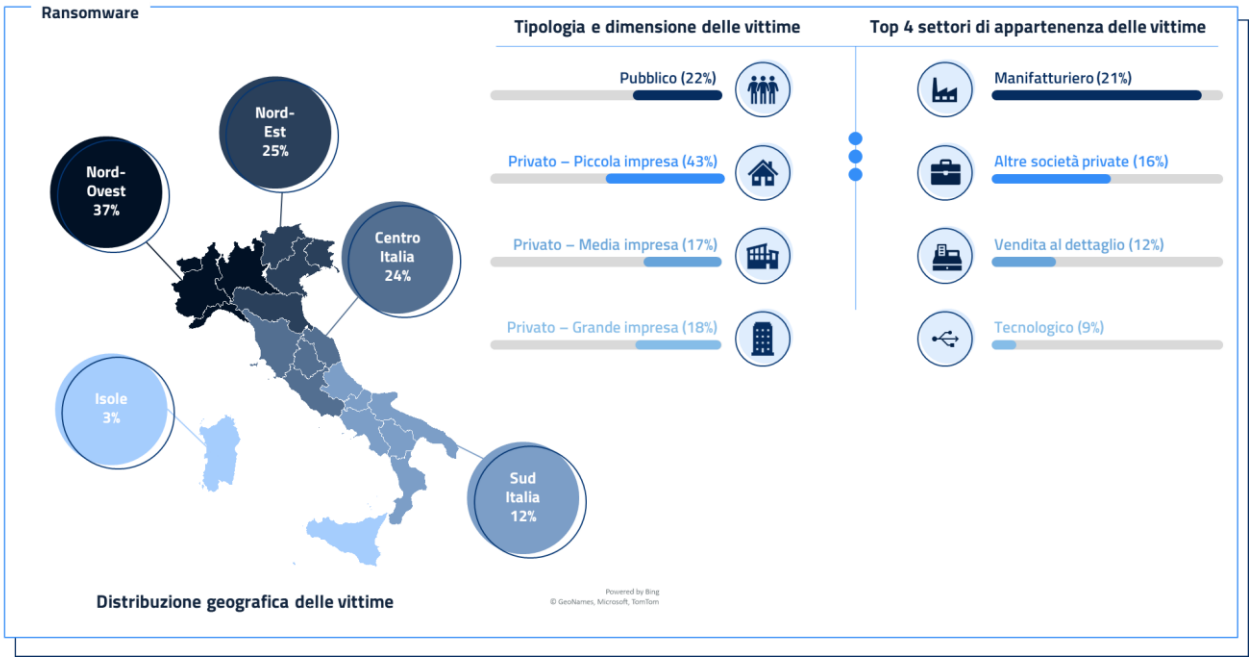

Figura 2: Distribuzione geografica e settoriale delle vittime di ransomware in Italia tra gennaio 2022 – novembre 2024

ATTACK STRATEGIES 2

Il presente capitolo offre una **panoramica sulle strategie di attacco prevalenti** relative alla minaccia ransomware, fornendo inizialmente un'analisi sulla loro evoluzione e successivamente un approfondimento sulle principali **tecniche e tattiche di attacco impiegate** suddivise per fase della *kill chain*. Il capitolo si conclude con una **panoramica su un caso studio di incidente ransomware**, per il quale sono presentate le attività di supporto fornite da ACN.

2.1 Evoluzione delle strategie di attacco

Secondo la pubblicazione "Ransomware Rebounds"[13] del 2024 di Mandiant, azienda statunitense leader nel settore della cybersecurity, negli ultimi anni gli attori criminali hanno privilegiato l'**aggiornamento di ransomware esistenti** piuttosto che sviluppare nuove famiglie di malware. Frequentemente, queste nuove varianti sono versioni di un ransomware preesistente per sistemi Windows, **adattate per compromettere anche altri sistemi operativi**. In precedenza, infatti, i *threat actors* si concentravano sullo sviluppo di payload per sistemi Windows, che costituiscono ancora il principale bersaglio degli attacchi ransomware[14], principalmente per motivi legati alla sua ampia diffusione e alla maggiore facilità di sviluppo.

Tuttavia, la diffusione di linguaggi di programmazione multipiattaforma ha significativamente facilitato lo sviluppo di payload per sistemi operativi diversi da Windows, rendendo più frequente lo sviluppo, anche simultaneo, di varianti di ransomware per sistemi di tipo Linux, ESXi, Unix, MacOS, BSD e Android[15].

[13] Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools – Mandiant, 2024

[14] RANSOMWARE - Evoluzione e misure di protezione - CSIRT Italia, 2021

[15] From Conti to Akira | Decoding the Latest Linux & ESXi Ransomware Families – SentinelOne, 2023

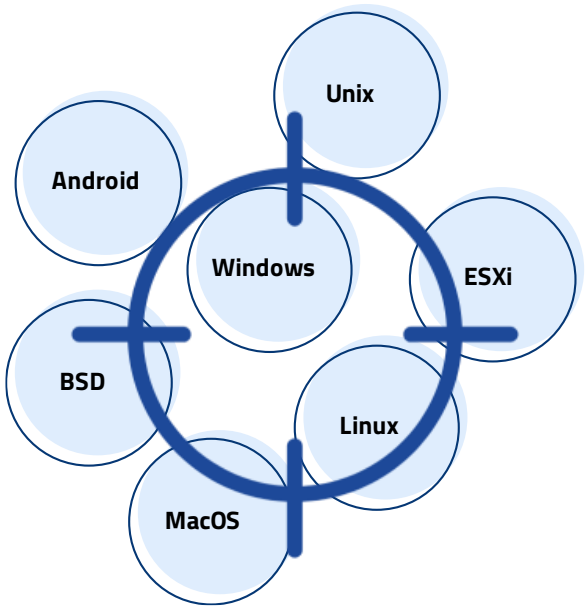

Figura 3: Alcuni dei sistemi operativi colpiti dalla minaccia ransomware

Oltre che per le differenze nell'attaccare sistemi operativi diversi, le famiglie di ransomware differiscono anche per **durata del processo di cifratura** dei dati, in base alla tipologia e all'implementazione degli algoritmi di crittografia utilizzati; processo che necessita di un lasso di tempo durante il quale l'attacco può essere rilevato e interrotto. Di conseguenza, gli attori criminali sviluppano frequentemente nuovi strumenti nel tentativo di ridurre il tempo richiesto che, per le principali famiglie di ransomware, può variare, per paragonabili quantità di dati da crittografare, da pochi minuti ad alcune ore[16].

Un esempio di tali tecniche è la **crittografia intermittente**[17], vale a dire la cifratura di una porzione del contenuto dei file della vittima. Questa tattica è stata osservata su molteplici famiglie di ransomware rilevanti, quali ad esempio Lockbit, ALPHV, PLAY e BlackBasta tra le altre[18].

La minimizzazione della durata delle operazioni offensive rappresenta una priorità per gli attori di minaccia, soprattutto considerando che il tempo medio di permanenza all'interno delle infrastrutture compromesse si è significativamente ridotto negli ultimi anni[19] grazie al potenziamento delle capacità di *detection* e delle competenze di risposta agli incidenti. Per gli attaccanti, la riduzione della finestra di esposizione consente di ridurre la probabilità di

[16] Most Common Types of Ransomware Today - Splunk, 2023

[17] Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection - SentinelOne, 2022

[18] Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection - SentinelOne, 2022

[19] M-Trends 2024: Our View from the Frontlines - Mandiant, 2024

rilevamento da parte dei sistemi difensivi, in particolare quelli basati sul monitoraggio di *pattern* comportamentali ed eventi nel tempo.

2.2 Tecniche e tattiche di attacco

Le strategie di attacco sono spesso meglio comprese attraverso lo studio della **cyber *kill chain***, un modello che rappresenta le fasi sequenziali di un attacco informatico, consentendo un'analisi sistematica e strutturata delle **metodologie operative** adottate dagli attori criminali[20]. Nel caso specifico del ransomware, la Figura 4 illustra le principali fasi e le caratteristiche distintive di un attacco tipo, che verranno approfondite e analizzate nel dettaglio nei paragrafi successivi.

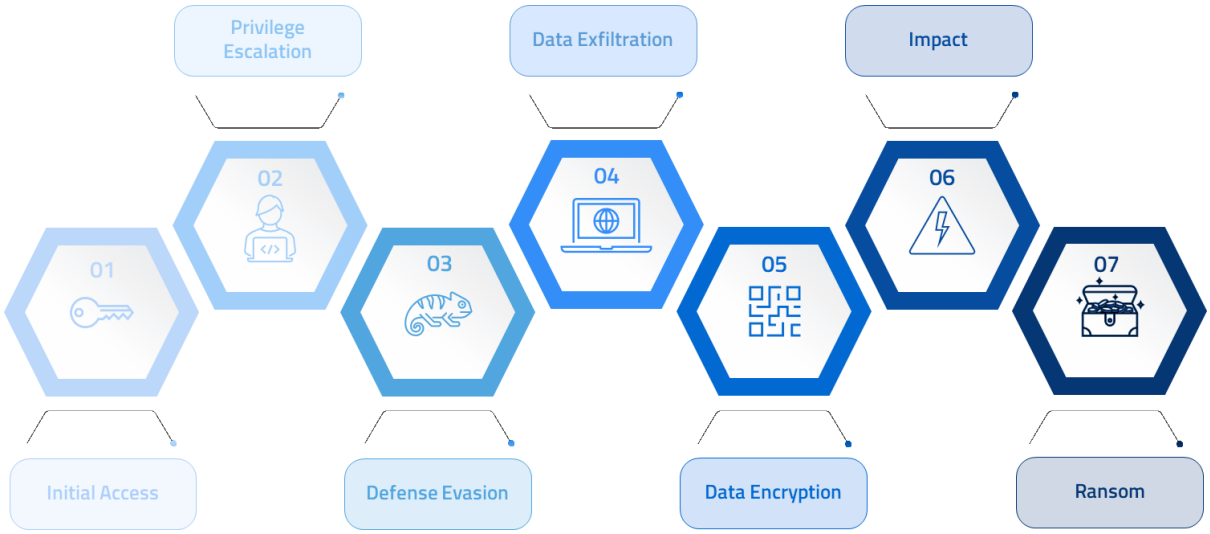

Figura 4: La kill chain di un attacco ransomware

Initial Access

A seguito di possibili attività di ricognizione condotte dall'attaccante per raccogliere informazioni sulla vittima, sui suoi dispositivi, sulle potenziali vulnerabilità, sui sistemi collegati e sui relativi sistemi di sicurezza, la prima fase di un attacco ransomware include tutte quelle tecniche che permettono, tramite lo **sfruttamento di alcuni vettori di attacco**, un iniziale accesso ai sistemi della vittima[21].

I vettori di compromissione iniziale del ransomware sono molteplici e non è sempre possibile determinare con precisione quale sia responsabile di una specifica infezione. Questa informazione, infatti, risulta spesso difficilmente tracciabile, sia per la possibile latenza del

[20] What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, 2022

[21] Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK®, 2019

ransomware nel sistema compromesso, sia per la potenziale reticenza della vittima nel condividere questa informazione, nel timore che lo stesso vettore possa essere sfruttato nuovamente da altri attori criminali. Si possono tuttavia identificare **tre principali vettori di attacco** della minaccia: il phishing, lo sfruttamento di vulnerabilità e l'utilizzo di credenziali compromesse.

Phishing

Il **phishing** rappresenta una tecnica di social engineering in cui un utente viene contattato, tramite e-mail o altri strumenti di messaggistica, da un attore di minaccia con l'obiettivo di indurre la vittima all'esecuzione di codice malevolo o all'accesso a risorse artefatte. Sfruttando leve psicologiche e inducendo stati emotivi di urgenza e preoccupazione, le campagne di phishing si focalizzano tipicamente su tematiche quali pagamenti da effettuare o ricevuti, ordini effettuati tramite piattaforme di *e-commerce*, documenti attesi o richiesti e comunicazioni apparentemente provenienti da organizzazioni autorevoli e riconosciute.

Il phishing costituisce uno dei vettori iniziali più comuni all'interno di una catena d'attacco informatico per la sua **bassa complessità, i costi contenuti e l'alta profittabilità**. In tempi recenti, poi, l'integrazione di strumenti basati sull'intelligenza artificiale e sui *Large Language Models* (LLM) ha reso l'elaborazione di e-mail di phishing estremamente più efficace e persuasiva. Difatti, se la creazione da parte di un attaccante di e-mail di phishing credibili e sviluppate su misura per una specifica vittima (*spear phishing*) può richiedere in media 16 ore, strumenti di intelligenza artificiale possono **ridurre queste tempistiche a circa cinque minuti**[22]. Inoltre, la diffusione di phishing kits e di servizi di Phishing-as-a-Service nell'ecosistema cybercriminale a prezzi estremamente abbordabili ha consentito l'ampliamento dell'accessibilità di tale tecnica.

Sfruttamento di vulnerabilità

Una **vulnerabilità** di sicurezza costituisce una debolezza che un avversario può sfruttare per compromettere la riservatezza, la disponibilità o l'integrità di una risorsa. Lo **sfruttamento** di tale vulnerabilità identifica l'evento cyber in cui un attaccante tenta o riesce a sfruttare, sia attraverso internet sia mediante rete interna, le falle di sicurezza di un bene informatico al fine di accedervi e ottenerne il controllo illecitamente. Questa categoria comprende sia lo sfruttamento di **vulnerabilità note**, documentate sul database delle CVE (*Common Vulnerabilities and Exposures*), sia quello delle vulnerabilità non note, denominate "**0-day**".

[22] IBM X-Force Threat Intelligence Index 2024 – IBM, 2024

Lo sfruttamento di vulnerabilità presenti in una rete, in un sistema o in un'applicazione può realizzarsi mediante ***exploit kit***, ovvero un insieme di strumenti software appositamente progettati e utilizzati per eseguire e automatizzare molteplici tecniche e procedure di attacco finalizzate ad accedere, infettare e danneggiare i beni informatici del bersaglio. Sebbene questi strumenti vengano comunemente impiegati per sfruttare vulnerabilità già note, per le quali esistono dei *Proof of Concept* (POC), non tutti gli attori malevoli possiedono le competenze e le risorse necessarie per sfruttare vulnerabilità non note[23]. L'utilizzo di "0-day" è infatti spesso correlato alla capacità finanziaria dei gruppi criminali, che possono reinvestire i proventi illeciti **nell'acquisizione di exploit e POC per vulnerabilità "0-day"**, riuscendo così a compromettere anche organizzazioni dotate di elevati livelli di sicurezza cibernetica.

Utilizzo di credenziali compromesse

Gli attori criminali possono **acquisire e utilizzare credenziali di account legittimi** come vettore per condurre operazioni malevole, quali l'*escalation* dei privilegi, l'implementazione di meccanismi di persistenza, l'esfiltrazione di dati sensibili o l'esecuzione di codice non autorizzato.

L'acquisizione di tali credenziali è frequentemente correlata al ***credential scanning***, un evento cyber in cui un attore malevolo esegue una scansione sistematica per individuare credenziali di autenticazione vulnerabili, configurate inappropriatamente o esposte su un asset informatico.

Oltre al *credential scanning*, gli attaccanti possono ottenere credenziali compromesse e *logs* attraverso l'acquisizione di *infostealers*[24] nei mercati dell'ecosistema criminale o mediante ***Initial Access Brokers*** (IABs), entità specializzate nel compromettere i sistemi delle vittime per poi monetizzare gli accessi così guadagnati ad altri attori criminali[25].

Privilege Escalation

Questa fase della *kill chain racchiude* diverse attività strategiche: **l'implementazione di meccanismi di persistenza** (*Persistence*), **l'esecuzione movimenti laterali** *(Lateral Movement*), **l'ottenimento di permessi di sistema** di livello superiore (*Privilege Escalation*) e l'instaurazione di canali di **comando e controllo** (*Command and Control*). L'attore malevolo può orchestrare e

[23] Ransomware Retrospective 2024: Unit 42 Leak Site Analysis – PaloAlto, 2024
Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools – Mandiant, 2024

[24] IBM X-Force Threat Intelligence Index 2024 – IBM, 2024

[25] Initial Access Brokers How They're Changing Cybercrime – Center for Internet Security, NA

reiterare queste operazioni secondo sequenze variabili.

A seguito della compromissione iniziale dei sistemi target, l'attaccante implementa **tecniche di persistenza** per garantirsi l'accesso continuativo anche in presenza di contromisure quali reset, modifica delle credenziali o altre azioni difensive[26]. A tal fine, gli attori malevoli impiegano frequentemente **strumenti di accesso da remoto legittimi** (quali ad esempio Anydesk, MeshAgent, ScreenConnect, Teamviewer, Splashtop)[27], inclusi quelli nativi del sistema operativo, così come *tunneler* (quali ad esempio SystemBC), *proxy malware* e BEACON, il payload di Cobalt Strike utilizzato per stabilire connessioni al team server[28]. Non è infrequente l'implementazione simultanea di molteplici strumenti di accesso remoto nello stesso ambiente[29].

Per conseguire l'elevazione dei privilegi (*Privilege Escalation*), gli attaccanti possono ricorrere ai movimenti laterali, un insieme di metodologie finalizzate all'accesso, controllo ed esecuzione di codice tra le risorse della rete interna. Questa tecnica consente la progressione dal punto di accesso iniziale verso altri segmenti del network per identificare dati da esfiltrare o cifrare[30]. L'esecuzione di tali attività si avvale di diversi strumenti e protocolli, inclusi account compromessi o creati ad hoc dall'attaccante, oltre all'utilizzo di RDP, SSH e SMB[31].

Il conseguimento degli obiettivi operativi richiede spesso privilegi elevati sul sistema compromesso, rendendo l'elevazione dei privilegi (*Privilege Escalation*) una fase critica. Lo **sfruttamento di credenziali** valide rappresenta una tecnica prevalente, facilitata dall'impiego di strumenti accessibili come MIMIKATZ e LAZAGNE. Il repertorio di tecniche include inoltre lo sfruttamento di vulnerabilità, DPAPI, attacchi kerberoasting[32] e l'utilizzo di strumenti nativi del sistema operativo come PowerShell, RDP, SMB e SSH[33]. La pratica di ricorrere a componenti e strumenti messi a disposizione dal sistema operativo vittima per lo svolgimento dell'attacco prende il nome di ***Living-off-the-land*** (LOTL). Gli attacchi LOTL risultano essere più difficili da rilevare, in quanto utilizzano funzioni e componenti nativi del sistema operativo sviluppati per

[26] Persistence, Tactic TA0003 - Enterprise - MITRE ATT&CK®, 2019

[27] Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools - Mandiant, 2024

[28] Cobalt Strike | Defining Cobalt Strike Components & BEACON - Google Cloud Blog, 2021

[29] Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools - Mandiant, 2024

[30] Lateral Movement, Tactic TA0008 - Enterprise - MITRE ATT&CK®, 2019

[31] Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools - Mandiant, 2024

[32] Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools - Mandiant, 2024

[33] Lifecycle of a ransomware attack: Consolidation and preparation - CERT NZ, NA

scopi legittimi, e possono eludere quei sistemi di sicurezza che rilevano l'eventuale presenza di script o file malware noti[34].

Per orchestrare queste operazioni, l'attaccante stabilisce canali di comando e controllo (*Command and Control*) per mantenere la comunicazione con i sistemi compromessi all'interno della rete target. Oltre a Cobalt Strike[35], strumento ampiamente utilizzato in questo contesto, vengono impiegati anche Sliver e Brute Ratel.

Defense Evasion

La fase di *Defense Evasion* comprende l'insieme delle tecniche che un attore malevolo potrebbe utilizzare al fine di **minimizzare la propria rilevabilità** durante un attacco. Tali tecniche possono includere la disabilitazione dei sistemi di *logging*, l'elusione dei controlli anti-malware, l'eliminazione dei log di sistema[36], nonché la disattivazione degli strumenti di sicurezza e l'offuscamento del codice malevolo.

Ulteriori tecniche includono la compromissione di procedure di routine essenziali per il mantenimento della postura difensiva, come ad esempio l'inibizione della disconnessione degli utenti da un computer o il blocco dello spegnimento dei sistemi[37]. Gli attori malevoli procedono inoltre alla rimozione o alterazione degli artefatti generati all'interno dell'infrastruttura target, sia per eliminare gli indicatori della propria presenza sia per degradare l'efficacia delle contromisure difensive[38]. Inoltre, un attaccante potrebbe tentare l'elusione delle difese anche sfruttando processi legittimi e simulando pattern di traffico conformi alle baseline operative del sistema target[39].

Data Exfiltration

L'**esfiltrazione** comprende il framework tattico che gli attori malevoli implementano per l'estrazione non autorizzata di dati dall'infrastruttura target[40]. Il materiale esfiltrato viene successivamente monetizzato attraverso strategie estorsive o mediante la commercializzazione

[34] What Are Living Off the Land (LOTL) Attacks? - CrowdStrike, 2023
[35] Lifecycle of a ransomware attack: Consolidation and preparation - CERT NZ, NA
[36] Ransomware attackers down shift to 'Mid-Game' hunting in Q3 – Coveware, 2021
[37] Impair Defenses, Technique T1562 - Enterprise | MITRE ATT&CK®, 2023
[38] Indicator Removal, Technique T1070 - Enterprise | MITRE ATT&CK®, 2023
[39] Ransomware attackers down shift to 'Mid-Game' hunting in Q3 – Coveware, 2021
[40] Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®, 2019

su *leak site* dedicati.

L'esfiltrazione dei dati può essere **mirata o indiscriminata**: l'esfiltrazione mirata prevede una selezione strategica dei dati basata su parametri specifici, quali parole chiave di interesse, criteri tassonomici o attributi tecnici come dimensione e metadata temporali; l'approccio indiscriminato, per contro, si caratterizza per l'acquisizione massiva di dati in assenza di criteri selettivi[41].

L'analisi empirica evidenzia una **prevalenza delle operazioni di esfiltrazione indiscriminata**, dove gli attori malevoli prediligono una raccolta massiva preliminare seguita da processi di analisi e filtrazione successivi (tale approccio ha la conseguenza di una maggiore complessità delle attività di *impact assessment* e *incident reporting* per l'organizzazione target). Tuttavia, va tenuto in considerazione che **maggiore è la mole di dati che viene esfiltrata, più probabile è che l'attaccante venga rilevato.** Va tuttavia considerato il rapporto direttamente proporzionale tra il volume dei dati esfiltrati e la probabilità di rilevamento dell'operazione: ciò spiega perché la prassi operativa dominante preveda un'esfiltrazione graduale in orari non lavorativi[42], finalizzata all'elusione dei sistemi di *Data Loss Prevention*.

Gli attaccanti, ai fini dell'esfiltrazione, ricorrono frequentemente a **strumenti legittimi** quali Rclone, MEGASync, WinRar, 7Zip, FileZilla o WinSCP. Altri meccanismi di esfiltrazione includono il trasferimento dei file tramite strumenti di accesso remoto o l'upload diretto dei file su cloud tramite web browser[43].

Data Encryption

La **cifratura dei dati** consente agli attori malevoli di comprometterne la disponibilità sui sistemi target in un network[44]. Questa tecnica è la più facilmente associabile ad un attacco ransomware, anche se, come precedentemente illustrato, recentemente gli attaccanti utilizzano in maniera più sistematica **tecniche di attacco che non richiedono la crittografia dei dati**, limitandosi alla loro esfiltrazione o corruzione, o che prevedono una forma di crittografia meno onerosa, come nel caso della **crittografia intermittente**[45].

Ulteriori metodologie di cifratura includono la **crittografia remota**, una tecnica che sfrutta

[41] 2024 Unit42 incident response report – Palo Alto Networks, 2024

[42] Lifecycle of a ransomware attack: Consolidation and preparation - CERT NZ, NA

[43] Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools - Mandiant, 2024

[44] Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®, 2022

[45] Ransoms Without Ransomware, Data Corruption and Other New Tactics in Cyber Extortion – Sentinelone, 2022

endpoint compromessi e con inadeguati livelli di protezione al fine di criptare i dati su altri dispositivi connessi alla stessa rete[46]. L'analisi delle tattiche operative ha inoltre evidenziato lo sfruttamento di strumenti di cifratura legittimi (come Bitlocker), una strategia che consente l'elusione dei sistemi di rilevamento senza necessità di sviluppo di codice dedicato.

È significativo evidenziare l'esistenza di iniziative di contrasto come **No More Ransomware**[47], un progetto collaborativo che coinvolge la National High Tech Crime Unit della polizia olandese, l'European Cybercrime Centre di Europol, Kaspersky e McAfee. Questa piattaforma fornisce strumenti di decifratura specializzati per diverse varianti ransomware, incluse famiglie di particolare rilevanza come BLACKBASTA, RHYSIDA, LOCKBIT 3.0, AKIRA e RAGNAR.

Impact

Oltre all'impiego della crittografia, gli attori malevoli hanno sviluppato molteplici tecniche finalizzate ad amplificare l'efficacia dell'attacco (**impact**) sul sistema target, compromettendone l'integrità operativa o impedendone il funzionamento. Queste metodologie includono l'esecuzione di attacchi DDoS e strategie di alterazione (*data curruption*) o eliminazione dei dati.

La corruzione dei dati, in particolare, consente all'attaccante di compromettere la disponibilità delle risorse sul sistema target attraverso un processo più efficiente in termini di tempo e risorse rispetto alla crittografia. Gli attori malevoli frequentemente impiegano strumenti di corruzione successivamente all'esfiltrazione dei dati, con l'intento di esercitare pressione sulla vittima e incrementare la probabilità di successo della richiesta di riscatto. Inoltre, diversamente dalla crittografia, per la quale vengono elaborate chiavi di decrittazione, per la corruzione dei dati non c'è la possibilità di sviluppare strumenti o contromisure tecniche "dirette".

Una metodologia più sofisticata, denominata "**Triple Extortion**"[48], prevede la combinazione sinergica di attacchi ransomware e DDoS. In questo scenario, l'attacco DDoS viene condotto in parallelo all'offensiva ransomware per intensificare il senso di urgenza nella vittima, compromettendo ulteriormente l'operatività dei sistemi target. In aggiunta, l'attaccante può tentare di disabilitare i servizi deputati al ripristino del sistema, precludendo l'accesso ai backup e alle funzionalità di *recovery* disponibili[49].

[46] Prolific Ransomware Groups Intentionally Switch On Remote Encryption for Attacks, Sophos Finds - Sophos, 2023

[47] Il progetto è accessibile dal seguente link: The No More Ransom Project

[48] Defeating Triple Extortion Ransomware: The Potent Combo of Ransomware and DDoS Attacks - Akamai, 2023

[49] Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®, 2024

Una volta eseguite le azioni sugli obiettivi designati, l'attaccante tipicamente notifica alla vittima l'avvenuta compromissione del sistema, finalizzata alla richiesta di un riscatto. Tale comunicazione avviene attraverso diverse modalità, quali **l'invio di messaggi di posta elettronica** o la predisposizione di una ***ransom note*** sul sistema compromesso. In alcuni casi, l'aggressore può anche stampare la *ransom note* utilizzando le stampanti della stessa organizzazione target.

Le *ransom note*, generalmente sotto forma di file **in formato .txt o .pdf**, contengono l'annuncio dell'avvenuta crittografia e/o esfiltrazione dei dati dal sistema compromesso. Nel caso di sottrazione di informazioni, questi messaggi spesso elencano la tipologia dei dati sensibili acquisiti, come informazioni personali dei dipendenti, dati finanziari, proprietà intellettuale e codici sorgente. L'attaccante, tipicamente, prosegue poi minacciando la divulgazione delle informazioni sottratte qualora non venga corrisposto il pagamento richiesto.

In presenza di attacco ransomware con crittografia dei dati, l'aggressore, in taluni casi, può voler dimostrare il possesso della chiave di decodifica offrendo la decrittazione di un numero limitato di file.

Tipicamente la *ransom note* fornisce inoltre le istruzioni necessarie per stabilire un contatto con l'attore criminale. Queste istruzioni possono includere l'installazione del browser Tor e l'accesso, mediante link dedicato, a una piattaforma di messaggistica dove vengono fornite specifiche credenziali d'ingresso per ciascuna vittima. L'importo del riscatto può essere indicato direttamente nella *ransom note* o comunicato attraverso i canali di messaggistica predisposti.

In caso di accettazione del pagamento, il riscatto viene solitamente corrisposto in **criptovalute** attraverso wallet multipli, talvolta dedicati singolarmente a ciascuna vittima. Una volta ricevuto il pagamento, l'attaccante esegue una serie di operazioni e transazioni al fine di **aggregare e anonimizzare** i proventi[50], ricorrendo frequentemente a *cryptocurrency mixers*, servizi che combinano le criptovalute di diversi utenti per mascherarne l'origine[51].

Infine, le *ransom note* si concludono generalmente con l'avvertimento di non alterare autonomamente i dati compromessi e di evitare l'utilizzo di software di terze parti per la decrittazione.

[50] Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report – Palo Alto Networks, 2021

[51] Crypto Mixers and AML Compliance - Chainalysis, 2022

2.3 Caso studio e attività di supporto ACN

Nel corso delle sue attività reattive, nel 2023 il CSIRT Italia ha gestito un incidente ransomware contro un'azienda ospedaliera. L'incidente viene qui descritto come esemplificazione della *kill chain* finora illustrata, con l'obiettivo di fornire una maggiore consapevolezza sul comportamento della minaccia.

A seguito di possibili attività di **ricognizione** condotte dall'attaccante per raccogliere informazioni sulla vittima e i relativi sistemi di sicurezza, nel caso in esame l'attore criminale si è introdotto nei sistemi dell'azienda per **esfiltrare** e **cifrare** i dati e i sistemi, chiedendo un riscatto per la loro decodifica.

Le **fasi relative all'incidente sono rappresentate e descritte nel dettaglio in Figura 5**. Per la gestione dell'incidente, il CSIRT Italia è intervenuto *in loco* a supporto della vittima, raccogliendo le evidenze e conducendo l'analisi forense sui sistemi coinvolti. Sulla base delle evidenze raccolte, il CSIRT Italia ha definito un piano di attività finalizzate al **ripristino della piena efficienza dei servizi** ospedalieri impattati, e fornito le raccomandazioni necessarie **all'innalzamento della postura di sicurezza dell'infrastruttura**.

Per contribuire al rafforzamento della consapevolezza situazionale del personale tecnico dell'azienda ospedaliera, il CSIRT Italia ha inoltre organizzato delle **sessioni di formazione** riguardo all'identificazione e all'isolamento delle minacce, alla mitigazione degli impatti e al ripristino delle normali operazioni.

RANSOMWARE
Le fasi di un incidente reale

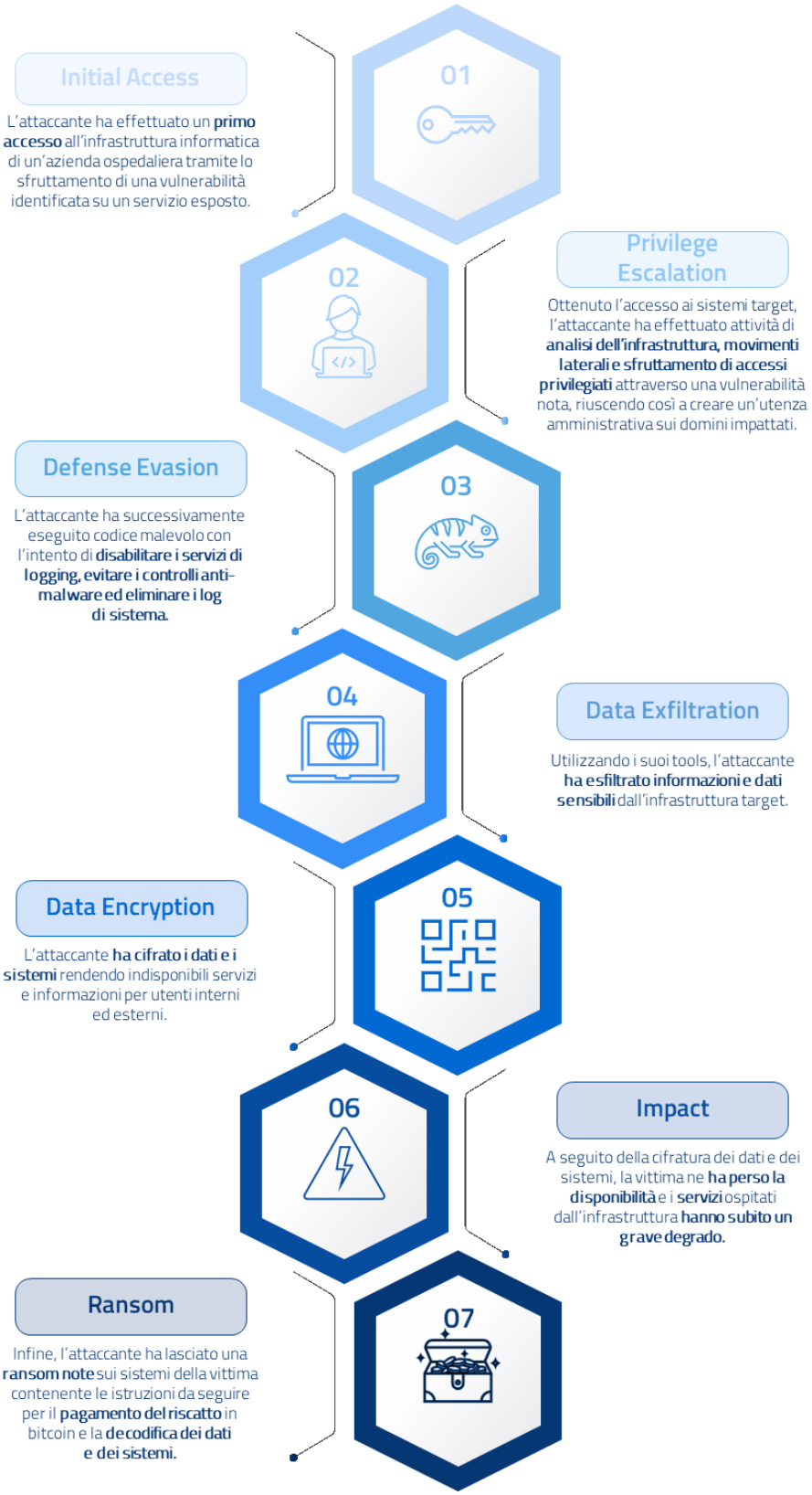

Figura 5: Le fasi di un incidente reale di ransomware

3 THREAT ACTOR

Per **"Threat Actor"** (TA) si intendono tutti quei soggetti in grado di originare o attuare una o più minacce potenzialmente in grado di arrecare danno alla Constituency. Gli attori operanti all'interno di questa categoria possono variare sulla base dei propri obiettivi, motivazioni, competenze, risorse, tattiche, procedure e tecnologie utilizzate per il raggiungimento dei propri scopi. Nel caso specifico della minaccia ransomware, i TA si organizzano spesso in **ransomware gang**, che verranno presentate in questo capitolo attraverso un'analisi dell'ecosistema criminale in cui operano, delle loro motivazioni, target e tecniche emergenti utilizzate.

3.1 Evoluzione dell'ecosistema criminale

L'evoluzione della minaccia ransomware ha comportato una riorganizzazione dell'ecosistema criminale, sostenuto dalla progressiva specializzazione degli attaccanti[52] e da una loro ristrutturazione in ***ransomware gang*** considerate oggi la forma organizzativa standard degli attori ransomware[53]. Questa organizzazione in gruppi criminali ha superato in frequenza il precedente modello organizzativo in singoli individui o piccoli gruppi, e prevede ora la definizione di ruoli e responsabilità interne per massimizzare le possibilità di successo di un attacco.

L'organizzazione in ransomware gang presenta molteplici vantaggi per gli attaccanti. In primo luogo, grazie alla suddivisione dei ruoli, ciascun attore criminale può **specializzarsi** in una specifica attività, ovviando a eventuali carenze tecniche su altre. In secondo luogo, le ransomware gang permettono agli attori criminali di **distribuire i costi anticipati** legati all'acquisto degli strumenti e delle infrastrutture necessarie allo svolgimento dell'attacco[54].

La specializzazione degli attaccanti ha permesso il raggiungimento di un grado di efficienza tale che alcuni gruppi hanno iniziato a offrire la propria infrastruttura anche ad utenti esterni al

[52] RANSOMWARE - Evoluzione e misure di protezione - CSIRT Italia, 2021

[53] Threat Landscape for Ransomware Attacks — ENISA, 2022

[54] Threat Landscape for Ransomware Attacks — ENISA, 2022

gruppo, spesso in cambio di una percentuale sul riscatto eventualmente ottenuto. È il modello del **RaaS**, che permette a operatori criminali specializzati di fornire codice malevolo preconfezionato, builder customizzati, servizi di back-office e infrastrutture di pagamento e distribuzione da loro perfezionate.

Gli attori che decidono di ricorrere ai servizi offerti dai gruppi RaaS prendono il nome di "**affiliati**", e ottengono la capacità di condurre attacchi ransomware senza la necessità di sviluppare in maniera autonoma il software e le infrastrutture. In cambio, gli "**operatori**" RaaS ricevono un contributo mensile da parte degli affiliati o una percentuale del riscatto ottenuto, che generalmente varia tra il 10-20%[55].

Risulta quindi evidente come l'avvento del RaaS abbia non solo notevolmente **abbassato le barriere d'ingresso**[56] economiche, tecniche e organizzative per la conduzione di attacchi ransomware, ma abbia anche fornito agli attaccanti un ulteriore livello di **protezione**[57]. Con l'aumento degli attori criminali che ricorrono allo stesso malware o si affidano alle stesse infrastrutture, risulta infatti più difficile distinguere i vari attaccanti fra loro. Questo risulta essere per gli attaccanti un vantaggio molto importante, soprattutto se si tengono in considerazione lo sviluppo di **partnership internazionali per la lotta al ransomware**, come l'International Counter Ransomware Initiative (CRI)[58] e il crescente numero di **operazioni che le forze dell'ordine** conducono contro di essi, utilizzando nuove strategie come la diffusione delle chiavi di decrittazione e la divulgazione pubblica dell'identità di attori di spicco nell'ecosistema del ransomware[59].

Nonostante questi benefici, l'appartenenza a gruppi RaaS può esporre gli affiliati al rischio di essere identificati a seguito di **operazioni di infiltrazione o sequestro degli asset** da parte delle forze dell'ordine.

Per evitare di attirare l'attenzione di questi ultimi, alcuni operatori RaaS definiscono delle **regole interne** sui target considerati legittimi e quelli da evitare, una categoria che include frequentemente le infrastrutture nazionali critiche. Di rado, tuttavia, alcuni gruppi criminali decidono di abbandonare questa regola come ritorsione nei confronti di azioni di polizia sempre più assertive; difatti alcuni attacchi contro infrastrutture critiche e sanitarie, soprattutto negli

[55] Threat Landscape for Ransomware Attacks — ENISA, 2022

[56] RANSOMWARE - Evoluzione e misure di protezione - CSIRT Italia, 2021

[57] Threat Landscape for Ransomware Attacks — ENISA, 2022

[58] L'iniziativa è accessibile al seguente link: International Counter Ransomware Initiative (counter-ransomware.org)

[59] U.S. Charges Russian National with Developing and Operating LockBit Ransomware - United States Department of Justice, 2024

Stati Uniti, vengono talvolta attribuiti a questa dinamica.

La diffusione del RaaS ha permesso la proliferazione di numerosi gruppi criminali, che si sono andati espandendo nel numero di affiliati. Per gli operatori, tale fenomeno ha comportato la necessità di vigilare sull'utilizzo che viene fatto degli strumenti messi a disposizione e quindi di rendere il **processo di selezione e reclutamento** più stringente. A seconda del livello di intenzionalità e selettività di tale processo, i gruppi RaaS si distinguono in **pubblici, ristretti** o **privati**[60].

Nei primi, il processo di reclutamento di nuovi affiliati è pubblicizzato principalmente su forum nel dark web attraverso post degli operatori RaaS che presentano i servizi offerti e illustrano le condizioni per poterne usufruire (generalmente il pagamento di un deposito e l'accettazione di condizioni per l'affiliazione al gruppo)[61].

Nei gruppi **RaaS ristretti**, agli aspiranti affiliati può essere richiesto di condividere prove di precedenti collaborazioni con altri gruppi RaaS e di riscatti precedentemente ottenuti, di essere in possesso di personale raccomandazione da parte di attori criminali già affiliati al gruppo o di poter vantare determinati indicatori reputazionali nell'ecosistema criminale[62].

I gruppi **RaaS privati**, invece, tendono a non pubblicizzare i propri servizi su forum e si affidano a canali confidenziali e privati per il reclutamento. Spesso la creazione di gruppi RaaS coincide con la chiusura di altri gruppi da parte delle forze di polizia, fornendo agli attori criminali un ambiente dove continuare a operare lontano dall'attenzione pubblica[63].

3.2 Analisi delle motivazioni e dei target

Gli attacchi ransomware vengono generalmente condotti con l'obiettivo di **ottenere un ritorno economico.** Le vittime vengono identificate in maniera **opportunistica** poiché possiedono caratteristiche che le rendono attaccabili, quali **particolari vulnerabilità** dal punto di vista della sicurezza cibernetica, o un'ampia disponibilità economica che garantirebbe agli attori criminali di massimizzare il valore del riscatto.

Tuttavia, identificare con certezza le motivazioni di un attaccante è spesso difficile, poiché alcuni attori possono ricorrere a strumenti e metodologie di attacco proprie di cyber criminali per mascherare il loro reale intento, quale ad esempio la conduzione di **campagne di spionaggio o**

[60] Fourth edition of the Franco-German Common Situational Picture – ANSSI-BSI, 2021
[61] Fourth edition of the Franco-German Common Situational Picture – ANSSI-BSI, 2021
[62] Fourth edition of the Franco-German Common Situational Picture – ANSSI-BSI, 2021
[63] Fourth edition of the Franco-German Common Situational Picture – ANSSI-BSI, 2021

destabilizzazione[64].

Sarebbe questo il caso di Threat Actor **Nation-State sponsored**, ovvero un Threat Actor sponsorizzato, apertamente o segretamente, da un ente statale di cui ne segue, anche parzialmente, le direttive a vantaggio di risorse significative (e.g.: compensi, strumenti, competenze, informazioni, etc.).

Distinguere fra cyber criminali e gruppi Nation-State sponsored è di conseguenza reso difficoltoso sia dalla strategia dei gruppi Nation-State di ricorrere a strumenti propri dei cyber criminali che dal **livello di sofisticazione** acquisito da questi ultimi[65]. Esempi di campagne ransomware attribuite da alcuni Stati a Threat Actor Nation-State sponsored sono WannaCry e NotPetya, entrambe emerse nel 2017[66]. Questa convergenza nelle tecniche da parte dei cyber criminali e delle organizzazioni Nation-State sponsored risulta più evidente dal 2022, in relazione all'evoluzione del conflitto in Ucraina[67].

Poiché gli attacchi ransomware sono nella maggior parte di natura opportunistica, non vi è generalmente da parte degli attaccanti una predilezione per un determinato tipo di settore produttivo. Nel caso delle campagne di ***Big Game Hunting***, le vittime sono spesso organizzazioni di grandi dimensioni con notevoli risorse finanziarie. In altri casi, le vittime sono scelte perché possiedono delle vulnerabilità di sicurezza che le rendono attaccabili, come ad esempio la presenza di dispositivi perimetrali o servizi esposti ad internet e vulnerabili.

Di conseguenza, e soprattutto nel caso di campagne ransomware non mirate, nessuna vittima è risparmiata in base al suo settore di attività economica o alla sua area geografica di provenienza. È tuttavia possibile notare come molteplici ransomware gang evitino, per regolamento interno, di colpire enti o organizzazioni provenienti da Stati appartenenti al *Commonwealth of Independent States* (CIS).

3.3 Tecniche emergenti

Le tecniche di esfiltrazione ed estorsione degli attori criminali sono in costante evoluzione. Di recente, gli attaccanti si sono concentrati prevalentemente sulla ricerca di specifiche informazioni

[64] Cyber threat bulletin: Modern ransomware and its evolution - Canadian Centre for Cyber Security, 2020
[65] Ransomware attacks, all concerned - How to prevent them and respond to an incident – ANSSI, 2021
[66] Modern Ransomware and Its Evolution – Canadian Centre for Cyber Security, 2020
Indicators Associated With WannaCry Ransomware - CISA, 2018
Petya Ransomware - CISA, 2018
[67] Cyber Threat Overview – ANSSI, 2023

sui sistemi della vittima quali documenti relativi all'eventuale **stipula di polizze assicurative**[68] o dati relativi ad eventuali **non conformità della vittima rispetto alle normative vigenti**. Queste informazioni vengono successivamente utilizzate dagli attori criminali per massimizzare le richieste di riscatto e applicare pressione sulle vittime.

In particolare, le informazioni relative all'eventuale non conformità alle normative vigenti viene spesso utilizzata per minacciare le vittime di **segnalazione alle autorità competenti** in caso di non pagamento[69], mentre le informazioni relative alla stipula di polizze assicurative contro il rischio ransomware permette agli attaccanti di aumentare la richiesta di riscatto, una tendenza che verosimilmente spinge le richieste di riscatto fino al massimo coperto dalle assicurazioni.

Un'altra tecnica emergente degli attori criminali riguarda la loro crescente tendenza a **esfiltrare e vendere i dati piuttosto che cifrarli**. Difatti, alcuni attaccanti hanno iniziato a rifiutare riscatti, in sede di negoziazione, nella convinzione di poter monetizzare maggiormente dalla vendita dei dati della vittima che dal pagamento del riscatto.

Questo è dovuto alla profittabilità dei dati e all'onerosità del processo di crittografia, che talvolta spingono gli attori criminali anche a rinunciare del tutto all'utilizzo di malware per la cifratura dei dati sul sistema vittima. Questa pratica prende il nome di attacco ransomware "***encryption-less***"[70], che riduce significativamente i tempi e le risorse necessarie per condurre l'attacco oltre che ridurre il rischio di conseguenti azioni delle forze di polizia[71].

Alcuni attori criminali hanno, per ragioni simili, iniziato a utilizzare malware sviluppato per **corrompere i file** in seguito all'esfiltrazione, invece che cifrarli, in quanto strumenti più facilmente sviluppabili, meno onerosi, non soggetti al possibile sviluppo di chiavi di decrittazione ma comunque capaci di impedire alla vittima l'accesso ai file[72].

Ulteriori tecniche che nel futuro potrebbero essere capaci di influenzare il panorama della minaccia ransomware riguardano l'utilizzo di strumenti basati sull'**Intelligenza Artificiale** (IA) e su **Large Language Models** (LLMs) per fini criminali. Simili strumenti possono essere usati per automatizzare lo sviluppo di malware permettendo, teoricamente, anche ad attori criminali senza elevate competenze tecniche di condurre attacchi sofisticati.

Guardando tuttavia allo stato dell'arte di queste tecnologie, lo sviluppo di malware sofisticati e capaci di svolgere anche le fasi più delicate della *kill chain*, quale l'evasione delle difese, richiede

[68] Cyber Insurance and the Ransomware Challenge - Royal United Services Institute, 2023

[69] Ransomware group reports victim it breached to SEC regulators - Ars Technica, 2023

[70] The Rising Threat of Encryption-less Ransomware Attacks - F5, 2023

[71] Ransomware gangs ditch encryption, embrace data extortion – Axios, 2023

[72] Ransoms Without Ransomware, Data Corruption and Other New Tactics in Cyber Extortion – SentinelOne, 2022

ancora una certa competenza tecnica da parte dell'attore criminale, che deve mostrarsi capace di comprendere e migliorare il malware sviluppato dai LLMs. Ciononostante, strumenti basati su tali linguaggi e sviluppati per fini criminali sono **già diffusi nell'ecosistema criminale**[73] e utilizzati prevalentemente per lo sviluppo di e-mail di phishing credibili e specifiche per la vittima in questione[74].

[73] New report finds that criminals leverage AI for malicious use – and it's not just deep fakes – Europol, 2020

[74] The near-term impact of AI on the cyber threat – NCSC, 2024

4 RACCOMANDAZIONI GENERALI

Proteggere i propri asset dalla minaccia ransomware richiede l'adozione di **misure preventive**, nonché il possesso delle capacità necessarie a **gestire un incidente** di tipo ransomware. Al fine di innalzare il livello di resilienza dei soggetti nazionali alla minaccia, questo capitolo presenta delle **raccomandazioni e contromisure generali**, identificate grazie all'esperienza dell'Agenzia nel supportare la gestione degli incidenti anche di tipo ransomware, nonché alla raccolta e razionalizzazione delle informazioni presentate in precedenti pubblicazioni[75].

Tali raccomandazioni non sono ugualmente applicabili ad ogni contesto e le contromisure da adottare possono variare in base alle specifiche caratteristiche della minaccia.

Queste raccomandazioni rappresentano quindi **azioni proattive largamente applicabili** volte a innalzare le capacità degli stakeholder di prevenire e mitigare l'esposizione al rischio della minaccia ransomware.

4.1 Raccomandazioni e contromisure

Le raccomandazioni e le contromisure qui proposte sono articolate in tre tipologie, vale a dire raccomandazioni che riguardano i **processi e le strategie**, raccomandazioni relative alle **soluzioni di sicurezza** e raccomandazioni relative ai **controlli di sicurezza**.

[75] Si vedano, ad esempio, RANSOMWARE - Evoluzione e misure di protezione - CSIRT Italia, 2021 e RANSOMWARE - Misure di protezione e organizzazione dei dati per un ripristino efficace - CSIRT Italia

Figura 6: Tipologie di raccomandazioni e contromisure

Le prime mirano a innalzare il livello di sicurezza nei confronti della minaccia ransomware fornendo indicazioni circa la preparazione, il testing e l'aggiornamento di **politiche organizzative, piani di risposta e strategie di recovery e gestione del rischio**. Una rappresentazione di tali raccomandazioni è riportata in Figura 7 a seguire.

Figura 7: Raccomandazioni relative ai processi e alle strategie

Le raccomandazioni relative alle soluzioni di sicurezza forniscono indicazioni circa gli strumenti e le **soluzioni tecnologiche da adottare** ai fini di migliorare la capacità di **tracciare gli eventi** di sicurezza, ridurre l'impatto di un eventuale incidente ransomware e **monitorare il perimetro** delle organizzazioni. Una rappresentazione di tali raccomandazioni è riportata in Figura 8 a seguire.

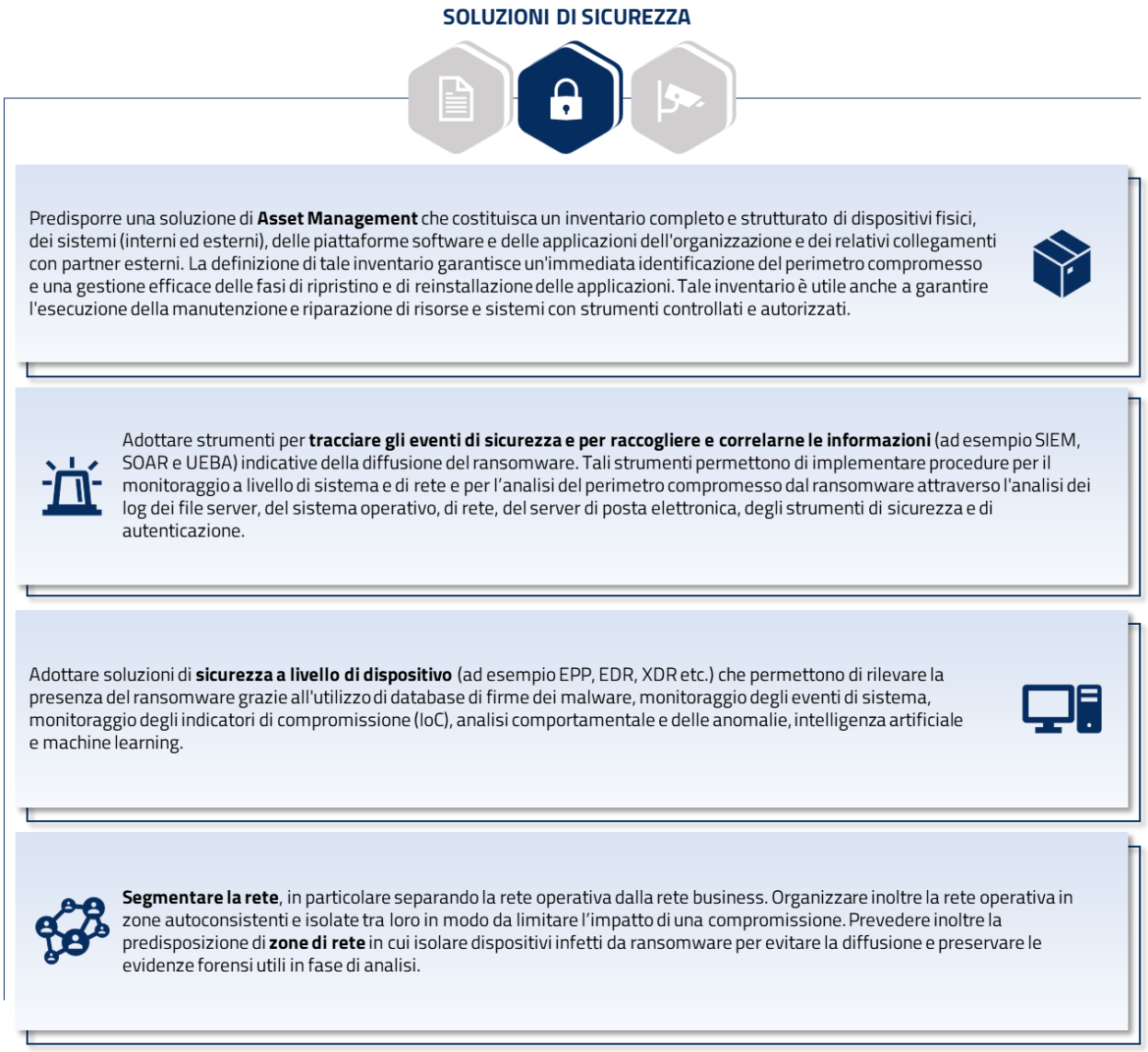

Figura 8: Raccomandazioni relative alle soluzioni di sicurezza

Le raccomandazioni relative ai **controlli di sicurezza**, infine, forniscono indicazioni circa determinate misure di sicurezza e processi tecnici da implementare ai fini di limitare i **punti di accesso vulnerabili** nel perimetro, **proteggere i dati sensibili** e adattare la propria **postura difensiva** in risposta alle evoluzioni della minaccia ransomware e del panorama delle vulnerabilità. Una rappresentazione di tali raccomandazioni è riportata in Figura 9 a seguire.

Figura 9: Raccomandazioni relative ai controlli di sicurezza

ALLEGATO

ATTIVITÀ DI RISPOSTA AGLI INCIDENTI RANSOMWARE

Il presente allegato fornisce, a titolo **esemplificativo e non esaustivo**, indicazioni di mero ausilio alle attività di risposta ad un incidente di tipo ransomware. Queste attività sono frutto dell'esperienza dell'Agenzia nella risposta agli incidenti e sono formulate per essere applicabili ad un'ampia platea di organizzazioni.

L'effettiva risposta agli incidenti dovrà essere adattata alle caratteristiche specifiche della minaccia e dell'organizzazione vittima. Il presente allegato non esonera le organizzazioni vittima da eventuali obblighi di notifica degli incidenti agli organi istituzionali competenti, come CSIRT Italia[76].

Le attività di risposta a un incidente ransomware sono qui strutturate in **cinque fasi**, modellate a partire dallo standard "NIST IR 8374 Ransomware Risk Management[77]" e dal "Computer Security Incident Handling Guide" definito dal Framework NIST SP 800-61 Rev.2[78].

Analisi

In questa fase si procede con l'analisi dello scopo e dell'impatto dell'incidente al fine di individuare il perimetro compromesso e le caratteristiche del ransomware. La fase di **Analisi** mira alla ricostruzione della causa principale dell'incidente di sicurezza e dell'ordine cronologico degli eventi correlati. Tale analisi informa le successive attività di contenimento e recupero, nonché permette di condividere informazioni specifiche con stakeholder e organi preposti.

[76] Sul sito di CSIRT Italia è disponibile un modulo da compilare in caso di incidente: Notifica incidente | Portale Segnalazioni

[77] Ransomware Risk Management: A Cybersecurity Framework Profile – NIST, 2022

[78] Computer Security Incident Handling Guide - NIST SP 800-61 Rev.2

Contenimento

Il **Contenimento** rappresenta la fase di gestione dell'incidente in cui vengono attuate le attività per contenere l'attacco, ridurre i danni e predisporre le fasi successive. Per un efficace contenimento è fondamentale identificare il principale meccanismo di propagazione del malware utilizzato dall'attaccante. Per procedere alle fasi successive è determinante identificare le tecniche sfruttate dall'attore malevolo per l'accesso, il movimento laterale e la persistenza nei sistemi target.

Recovery

La fase di **Recovery** ha l'obiettivo di ripristinare i sistemi, i servizi e il loro funzionamento in base alle risorse a disposizione.

Hardening

La fase di **Hardening** ha l'obiettivo di innalzare la postura di sicurezza dell'organizzazione, rafforzando le capacità di monitoraggio, revisionando i processi e le procedure, consolidando eventuali servizi implementati in emergenza e implementando le raccomandazioni identificate.

Comunicazione

Le attività di **Comunicazione** permettono alla vittima di adempiere ad eventuali obblighi normativi di notifica incidente, di mantenere informati i propri stakeholder interni ed esterni sull'evoluzione dell'attacco, e di gestire eventuali interazioni con terze parti secondo la strategia di comunicazione definita.
Le attività di dettaglio da compiere nelle fasi qui espresse sono rappresentate in Figura 10.

RANSOMWARE

Attività di risposta agli incidenti

Fase	
0	Un **sospetto incidente per attacco ransomware** si innesca per una o più delle seguenti condizioni: - rilevazione su parco macchine di ***ransom note*** **e/o impatti di fermo o prestazionali** su un insieme esteso del parco macchine; - **notizia su *leak sites* pubblici e/o comunicazioni** ricevute direttamente che indicano una possibile compromissione di informazioni; - **notifica** da parte dei sistemi di detection.
1	**L'Incident Manager** (IM) dà inizio alle attività di risposta all'incidente in base ai piani predisposti, valutando l'impatto, anche potenziale, dell'attacco in termini di servizi erogati ed in termini di conseguenze sugli asset. Si attiva, se necessario, il piano di **business continuity**. L'IM organizza, inoltre, il team di risposta, assegna le responsabilità e monitora l'implementazione delle procedure e delle strategie. Ogni implementazione di nuova tecnologia viene sospesa dall'IM fino alla chiusura dell'incidente.
2	**Distribuire o completare la copertura dell'EDR** e istituire un servizio minimo di monitoraggio laddove non presente.
3	Avviare le attività di analisi al fine di **confermare l'eventuale incidente** di sicurezza e raccogliere i primi parametri relativi all'estensione anche temporale dell'evento cyber.
4	**Analizzare le informazioni a disposizione**, identificando i sistemi, applicativi ed account coinvolti nell'incidente nonché le aree di rete particolarmente impattate. Analizzare inoltre il meccanismo di propagazione e di comunicazione con l'esterno (per esfiltrazione e controllo). Raccogliere le informazioni necessarie alla notifica **dell'incidente** in linea con le normative vigenti, effettuando anche una valutazione degli impatti sui servizi erogati.
5	Se possibile, avviare attività di **contenimento immediate** per disinnescare il meccanismo di propagazione. Avviare il processo di segnalazione esterna verso gli **organi istituzionali competenti** (Polizia Postale, CSIRT Italia, il Garante per la Protezione dei Dati Personali ed altri enti in base alle normative vigenti) inviando aggiornamenti secondo quanto definito.
6	Avviare le **attività di analisi**. I dati provenienti dall'analisi devono essere utilizzati per alimentare i meccanismi di monitoraggio e risposta. Dare anche inizio all'attività di **analisi forense** predisponendo il supporto alle autorità per l'acquisizione, la conservazione conforme e l'identificazione di tracce in immagini di dischi, memoria, *logs* e altri artefatti. Avviare, secondo le strategie di comunicazione preposte, i **processi di comunicazione interni ed esterni** (stakeholder, fornitori, clienti e dipendenti).
7	**In caso di ransomware human-operated**: • disabilitare ove possibile le utenze compromesse; • verificare la consistenza dei backup dei domain controller e di eventuali altri servizi critici in un ambiente isolato; • effettuare il reset di tutte le credenziali amministrative e di quelle coinvolte nell'incidente, resettare il ticket Kerberos (due volte) al fine di invalidare tutti i token emessi utilizzando l'account compromesso. Nel processo, assicurarsi di mantenere l'accesso all'utenza amministrativa; • procedere, infine, con l'applicazione di MFA sui sistemi esposti e condurre attività di hardening dei servizi di accesso remoto (quali VPN e tool di accesso remoto). **In caso di ransomware automatizzato**: • valutare se è possibile contrastare la propagazione del malware inibendo il meccanismo di replicazione, ad esempio isolando la rete, o distribuendo patch o regole sul sistema EDR; • bonificare eventuali account compromessi; • verificare la possibilità di chiudere in compartimenti separati aree logiche differenti di rete. Nell'impossibilità di eseguire azioni più specifiche disconnettere immediatamente i dispositivi infetti dal network, dall'internet e da altri dispositivi. Se non risulta possibile disconnettere i dispositivi infetti dal network, l'ultima opzione rimane quella di spegnerli, rischiando tuttavia di compromettere la possibilità di recuperare informazioni utili.
8	Condurre attività di **patching dei sistemi critici**, quali ad esempio firewall e domain controller.
9	**Salvare tutte le ulteriori informazioni acquisibili** sul malware e sulle modifiche eseguite dall'attaccante. Assicurarsi che le definizioni anti-virus siano aggiornate. Prima di rimuovere qualsiasi malware identificato, assicurarsi di registrarne le caratteristiche.
10	**Identificare e rimuovere ogni presenza dell'attaccante**, nonché eventuali meccanismi di persistenza, canali di esfiltrazione e canali di controllo dall'esterno che gli attaccanti potrebbero aver creato per assicurarsi di poter riaccedere e controllare la rete o il sistema colpito.

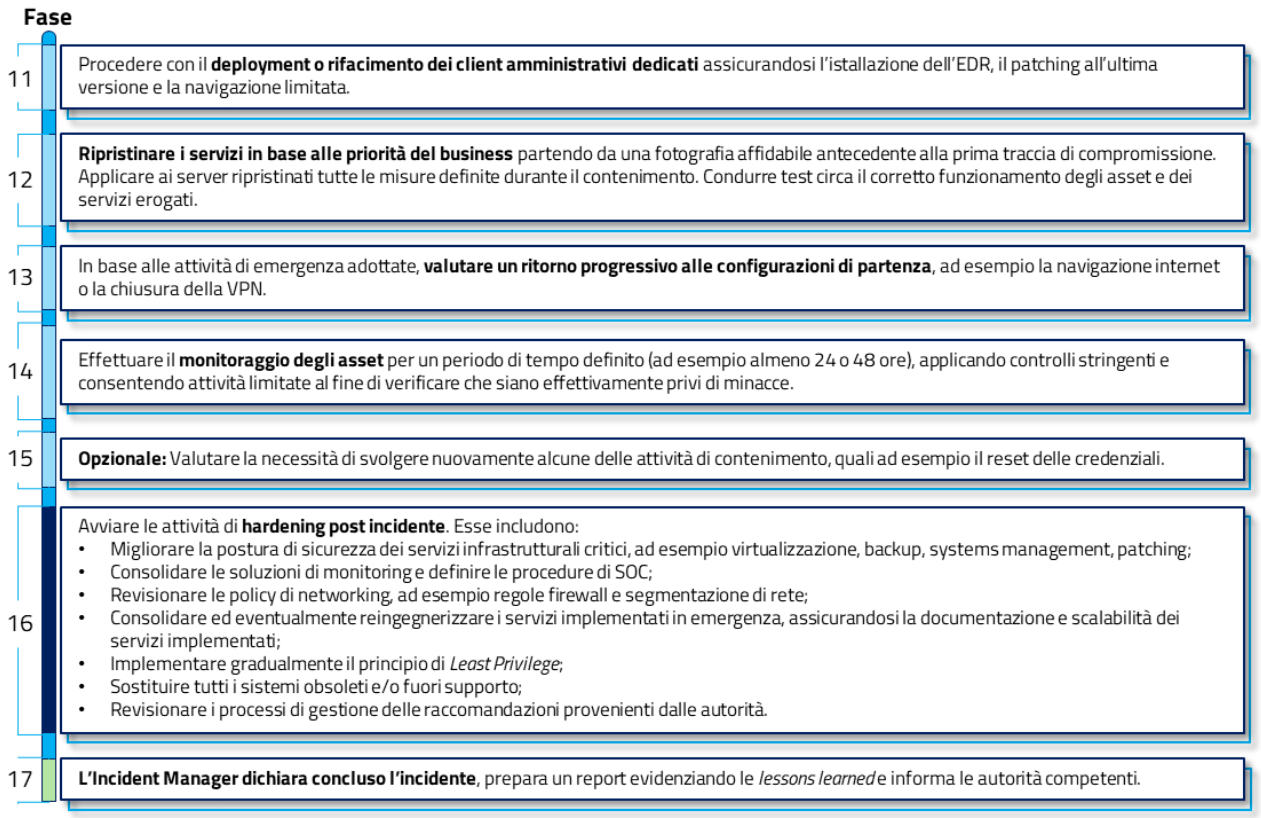

Figura 10: Le attività di risposta a un incidente ransomware

TLP:CLEAR

IN CASO DI INCIDENTE CONTATTA CSIRT ITALIA

Il **CSIRT Italia** è il centro operativo all'interno dell'Agenzia per la Cybersicurezza Nazionale (ACN) incaricato delle azioni di preparazione, prevenzione, gestione e risposta a eventi cibernetici.

La sua capacità di coordinare la risposta a incidenti cyber complessi gioca un ruolo fondamentale nella protezione degli asset strategici nazionali e nell'assicurare la disponibilità e l'affidabilità delle infrastrutture critiche.

In caso di incidente, compilare il modulo disponibile

https://segnalazioni.acn.gov.it/