UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Facoltà di INGEGNERIA

Corso di laurea magistrale in INGEGNERIA INFORMATICA

Corso di SICUREZZA INFORMATICA

a.a. 2021/2022

Diamond Model

A cura di

Andrea Silvestri

Sommario

Introduzione

Di seguito verrà presentata una breve sintesi del documento.

L'approfondimento corrente è pensato per fornire ai professionisti che operano in ambito di *cybersecurity* (es. *system administrators*) un modello che consenta di supportare efficacemente l'analisi e la prevenzione di *ransomware*, anche se è possibile astrarlo e applicarlo ad attacchi informatici generici.

Nell'elaborato intendo dimostrare che il *Diamond Model of Intrusion Analysis* è uno strumento efficace per i citati professionisti in quanto consente di analizzare i quattro componenti principali di ogni attacco e creare relazioni tra essi, nonché contestualizzare lo stesso nel luogo dell'avvenimento con l'obiettivo di chiarire le motivazioni e i fattori che hanno contribuito al suo successo.

Dopo un'introduzione sul tema *ransomware*, in particolare circa la tipologia *double extortion ransomware* seguirà una trattazione di alcuni casi di studio relativi a vicende realmente accadute.

Contesto

La sezione corrente è volta a fornire una breve introduzione sull'indagine effettuata.

Ransomware: definizione e tipologie

Definizione

Il *ransomware* è una tipologia di *malware* che tiene in ostaggio i dati sottratti da un dispositivo informatico e promette di restituirli soltanto previo pagamento di un riscatto (*ransom*). Il dispositivo vittima tipicamente subisce un processo di cifratura dei dati in esso contenuti così da renderlo inutilizzabile e causare disservizi.

Double extortion ransomware

Per aumentare la forza dell'attacco spesso i *ransomware* non solo criptano dati e sistemi ma minacciano la vittima di pubblicare in Rete le informazioni sottratte. Tale variante prende la denominazione di *double-extortion ransomware*.

Chiaramente, tale variante risulta essere estremamente pericolosa in quanto, oltre ai disservizi causati da un attacco consueto, viene lesa profondamente la *privacy* della vittima, esponendola a furti d'identità e attività illegali in genere.

Metodologia

Il capitolo contiene la descrizione dell'approccio Diamond Model.

Diamond model

Il *Diamond Model of intrusion analysis* (figura 1) è un modello di analisi di un attacco informatico che si avvale di una rappresentazione grafica a forma di diamante (da qui la denominazione) in cui si specifica che un **avversario** implementa una **capacità** su un'**infrastruttura** contro una **vittima**. Tali elementi sono chiamati **eventi** e, posti ai **vertici** del *diamond*, rappresentano le sue caratteristiche atomiche.

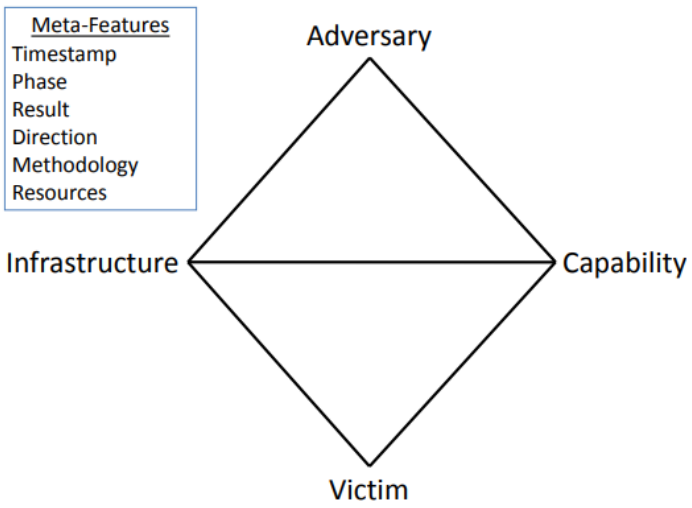


Figura 1. Il Diamond Model composto dai suoi quattro componenti principali (posti ai vertici) e collegati fra loro tramite bordi. Sono evidenziate anche le "meta-caratteristiche".

I vertici sono collegati fra di essi mediante **bordi** che evidenziano la relazione naturale tra le caratteristiche atomiche. Analizzando nel dettaglio ogni vertice ed esaminando le relazioni tra ciascuno di essi è possibile ottenere molteplici informazioni sull'avvenimento, sul contesto, sulle criticità che hanno consentito lo svilupparsi dell'evento e sulle operazioni dell'avversario al fine di implementare strategie difensive efficaci e prevenire accadimenti futuri.

Un evento descrive un passaggio di una serie di operazioni che l'avversario deve eseguire per raggiungere il proprio obiettivo. In quanto tali, gli eventi sono ordinati per fase in base alla coppia avversario-vittima in thread di attività che rappresentano il flusso delle operazioni di un avversario.

Sia gli eventi che i thread di attività sono elementi necessari per una comprensione completa dell'evento dannoso, in quanto una mitigazione più efficace e strategica richiede una nuova comprensione delle intrusioni stesse, non come eventi singolari, ma piuttosto come progressioni graduali.

Una volta stabiliti i thread di attività, gli eventi possono essere inseriti nei thread per identificare le campagne avversarie e riuniti in gruppi di attività per identificare eventi e minacce che condividono caratteristiche comuni. Tali gruppi di attività possono essere utilizzati per la correlazione automatizzata di eventi, nonché per opzioni e scenari di mitigazione del gioco e della pianificazione che stabiliscono piani di mitigazione strategici per contrastare l'avversario.

Casi di studio

Partendo da tale concetto il documento intende comprendere con precisione i fattori che hanno scatenato l'evento dannoso, le lacune che ne hanno impedito la mitigazione e, in seguito, cosa ha insegnato l'accaduto, quali cambiamenti sono stati attuati e quali contromisure si potevano e si dovranno attuare.

Di seguito verranno analizzati quattro casi di attacchi *Ransomware* realmente avvenuti. Le motivazioni che hanno portato alla scelta dei seguenti episodi riguardano principalmente:

- **impatto**; l'entità del danno e il numero di dispositivi e persone coinvolte sono stati enormi;
- **vicinanza temporale**; eccetto *WannaCry* che è avvenuto nel 2017 ed è stato riportato principalmente per l'enorme impatto a livello mondiale, i restanti casi di studio sono avvenuti nel corso del 2021 e hanno utilizzano tecniche evolute come la *double extortion*;
- **conseguenze**; gli effetti causati sono stati devastanti: in tutti gli episodi si sono rilevati disservizi gravi e protratti nel tempo con tempi di recupero estremamente lunghi.

WannaCry

Descrizione

WannaCry è stato un attacco globale avvenuto nel maggio 2017. Esso si è diffuso attraverso i computer con sistema operativo *Microsoft Windows* obsoleti o non aggiornati con le ultime *patches*. In particolare, i responsabili dell'attacco hanno sfruttato una debolezza di *Windows* già scoperta dalla *National Security Agency degli Stati Uniti* e per cui *Microsoft* aveva rilasciato, ancora nel mese di marzo, alcuni aggiornamenti di sicurezza. Come spesso accade, molti dispositivi non ricevevano gli ultimi aggiornamenti e ciò ha aumentato notevolmente la superficie di attacco a livello globale.

Inizialmente si pensava che l'attacco si fosse diffuso attraverso una campagna di *Phishing*. In seguito, si è notato che esso si basava su *EternalBlue*, che ha permesso a *WannaCry* di propagarsi e diffondersi, e su *DoublePulsar*, la *backdoor* che veniva installata sui computer compromessi.

Impatto

L'evento ha colpito circa 230.000 dispositivi in tutto il mondo coinvolgendo pesantemente 150 Paesi. In particolare, nel Regno Unito sono stati colpiti migliaia di ospedali e ambulatori del Servizio Sanitario Nazionale.

Applicazione del Diamond Model

Vittima

Le vittime sono tutti quei dispositivi (e, di conseguenza, gli utenti proprietari) che non hanno installato le *patches* di sicurezza contro *EternalBlue* rilasciate da Microsoft due mesi prima o che eseguivano sistemi obsoleti (anche se Microsoft aveva deciso di rilasciare le *patches* anche per questi). Tra le vittime troviamo specialmente il servizio sanitario nazionale (NHS) del Regno Unito, gli ospedali statunitensi, l'industria automobilistica (Nissan, Honda, Renault), Polizia cinese, alcune banche russe [1]

Capacità

WannaCry crittografa i dati dei sistemi infettati e richiede pagamenti di riscatto da $ 300 a $ 600 in Bitcoin. Il malware si propaga via rete verso altri sistemi che presentano la vulnerabilità descritta.

Quando raggiunge un sistema, utilizza

- l'exploit *EternalBlue* utilizzando la porta 445 (protocollo SMB, Server Message Block) per ottenere l'accesso al dispositivo;
- lo strumento *DoublePulsar* per installare una backdoor ed eseguire una copia di sé stesso.

In pochi secondi il ransomware crittografa tutti i file e aggiunge a ciascuno l'estensione *WNCRY*.

Per quanto concerne la crittografia, il ransomware è basato sull'utilizzo di RSA (come cifratura asimmetrica) e di AES (come simmetrica). In caso di infezione, utilizza le *cryptoAPI* del sistema operativo per geneare una coppia di chiavi RSA a 2048 bit. Inoltre, viene generata una chiave AES a 128 bit (in modalità Cipher Block Chaining) per la crittografia dei file della vittima. Queste chiavi simmetriche vengono quindi crittografate dalla chiave pubblica precedente [2].

Infrastruttura

Inizialmente si pensava che il malware si diffondesse tramite *e-mail* di *Phishing* contenente un link o un file malevolo che, una volta premuto, installa *WannaCry* sul sistema vittima. Successivamente si è scoperto che *WannaCry* si diffondeva soprattutto tramite un'operazione di *port scanning* verso la porta SMB esposta su Internet.

Secondo il *Diamond,* ciò costituisce un'**infrastruttura di tipo I** poiché gli aggressori diffondono l'attacco iniziale cercando i sistemi vulnerabili.

Avversario

Secondo un'indagine del Cyber Behavioral Analysis Center dell'FBI, il ransomware conteneva caratteri della lingua Hangul (usata in Corea). Inoltre, sono state reperite alcune informazioni riguardo l'utilizzo del fuso orario UTC+09:00, utilizzato in Corea. Infine, sono state trovate somiglianze di codice tra *WannaCry* e un precedente malware utilizzato da Lazarus Group nell'hacking di Sony e in una rapina in banca in Bangladesh, che era collegato alla Corea del Nord. Il 18 dicembre 2017, il governo degli Stati Uniti, insieme a Canada, Nuova Zelanda, Giappone e Regno Unito, hanno formalmente annunciato di considerare pubblicamente la Corea del Nord il principale colpevole dell'attacco *WannaCry* [3].

Meta caratteristica socio-politica

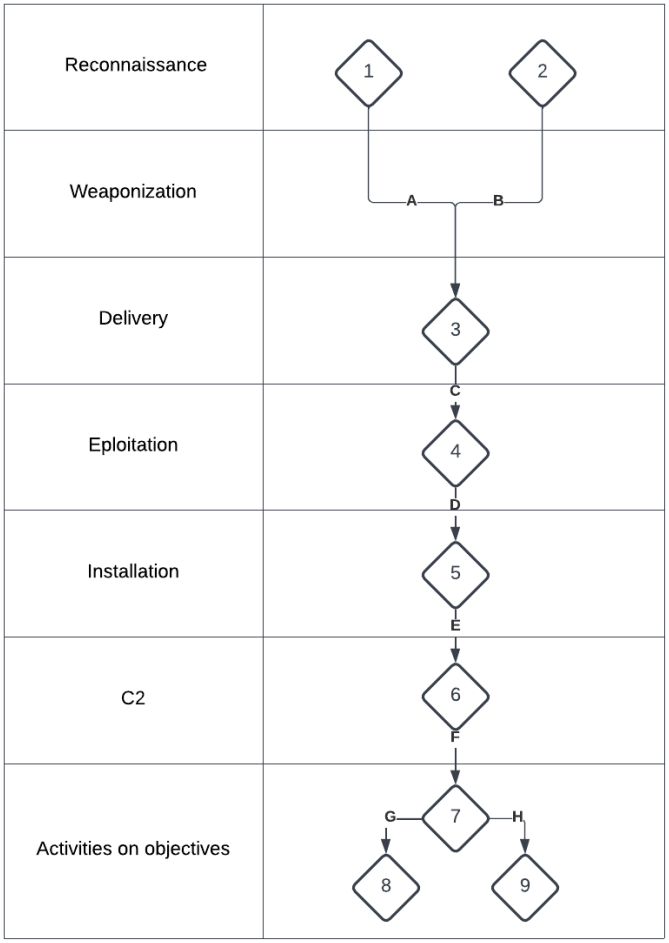
Dall'analisi delle transazioni nella blockchain è possibile comprendere quanti pagamenti del riscatto sono stati effettuati; in particolare, sono stati versati 54,43 bitcoin per un totale di 430 pagamenti e, pensando al gran numero di dispositivi infettati, in realtà è una cifra praticamente irrisoria.

Al contrario, secondo una stima della società *Symantec*, i danni causati dal ransomware in questione si aggirano attorno alla cifra di quattro miliardi di dollari a livello globale, in quanto oltre ad aver colpito privati e professionisti, sono state attaccate anche realtà critiche come il sistema sanitario britannico causando enormi disagi specialmente dovuti alla perdita di informazioni sensibili, cartelle cliniche e prenotazioni di sale operatorie.

Meta caratteristica tecnologica

WannaCry si diffonde principalmente mediante scansione delle porte relative al servizio SMB esposte pubblicamente sulla rete Internet e utilizza una scansione di un dominio HTTP (fino a quel momento inesistente) prima di avviare l'attacco. Quest'ultima tecnica viene denominata *kill switch* e viene utilizzata dall'attaccante per bloccare la diffusione del ransomware qualora ce ne fosse bisogno.

Riassumendo, l'esecuzione è schematizzata nei seguenti passaggi:



Evento	Ipotesi/attuale	Descrizione
1 (reconnaissance)	Attuale	L'attaccante effettua scansioni delle porte relative al servizio *SMB* esposte pubblicamente sulla rete Internet.
2 (reconnaissance)	Attuale	In alternativa, a mezzo *e-mail* di *phishing* o campagne di *spam* tenta di indurre le vittime ad aprire un messaggio malevolo contenente un trigger per avviare il ransomware.
3 (delivery)	Attuale	Il ransomware entra nel dispositivo rilevato ai passi precedenti attraverso le porte aperte.
4 (exploitation)	Attuale	Appena avviato, il ransomware controlla l'esistenza del dominio *www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com* utilizzato come killswitch; se esso non esiste, procede.
5 (installation)	Attuale	Il ransomware crea due chiavi di registro: ❖ *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Random>* con valore ***tasksche.exe*** ❖ *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Random>* con valore ***tasksche.exe*** e crea il servizio mssecsvc.exe per garantirne l'esecuzione: ❖ Nome servizio: ***mssecsvc2.0*** ❖ DisplayName: ***Servizio Microsoft Security Center (2.0)***. ❖ BinaryPath: ***<percorso di mssecsvc> -m security***
6 (C2)	Attuale	Il ransomware utilizza canali *Tor* crittografati per le comunicazioni di comando e controllo.
7 (action)	Attuale	Il ransomware genera due *threads*: uno si occupa della diffusione del malware all'interno della rete locale mentre l'altro si occupa della crittografia dei dati.
8 (action)	Attuale	Il primo thread esegue un processo che si occupa di enumerare le macchine vulnerabili all'interno della rete, tentando di connettersi alla porta 445; se il test ha esito positivo il ransomware contatta la directory ***\\<ip-address>\IPC$*** e tenta di installarsi sul dispositivo remoto.
9 (action)	Attuale	Il secondo thread avvia il servizio ***mssecsvc2.0*** precedentemente installato il quale esegue le seguenti attività: ❖ importa la chiave privata RSA utilizzata per la cifratura;

		❖ inizia a criptare i file contenuti nelle cartelle del profilo utente, quali Desktop e Raccolte, evitando gli eseguibili e i file già crittografati; ❖ esegue i comandi o ***taskkill.exe /f /im Microsoft.Exchange*** o ***taskkill.exe /f /im sqlserver.exe*** per spegnere eventuali databases e server di posta così da poter cifrare anch'essi; ❖ prepara il messaggio contenente le istruzioni da fornire all'utente per il pagamento del riscatto

Arco	**Confidenza**	**And/Or**	**Ipotesi/Attuale**	**Fornisce**
A	Media	And	Attuale	Fornisce informazioni sull'host da attaccare.
B	Media	And	Attuale	Fornisce informazioni sull'host da attaccare.
C	Alta	And	Attuale	-
D	Alta	And	Attuale	-
E	Alta	And	Attuale	-
F	Alta	And	Attuale	-
G	Bassa	And	Attuale	Identificazione di altri host nella rete (se presenti).
H	Media	And	Attuale	-

Colonial Pipeline

Descrizione

L'attacco alla *Colonial Pipeline* è iniziato il giorno 6 maggio del 2021 quando un gruppo di aggressori, proprietari del ransomware *DarkSide*, sono entrati nella rete del gruppo attraverso un account *VPN*.

Gli aggressori, agendo con un *ransomware double extortion*, hanno dapprima esfiltrato un'enorme quantità di dati per poi infettare la rete informatica; l'attacco ha colpito molti sistemi, inclusi quelli amministrativi e di gestione dell'oleodotto.

Applicazione del Diamond Model

Vittima

La vittima principale è stata la società *Colonial Pipeline* che ha chiuso i propri stabilimenti per circa sei giorni al fine di contenere l'impatto.

Dato che il Gruppo è uno dei principali fornitori di carburante degli Stati Uniti sono state influenzate anche altre organizzazioni, inclusa la difesa militare e l'industria aerea. Inoltre, a causa della minaccia di una carenza di carburanti, quattro stati (North Carolina, Virginia, Georgia e Florida) hanno dichiarato lo stato di emergenza.

Capacità

Il ransomware *DarkSide* utilizza uno schema di crittografia ibrido, basato sull'algoritmo *ChaCha20* combinato con l'algoritmo di cifratura a chiave pubblica RSA-1024. Inoltre, il ransomware viene differenziato in base al sistema operativo di destinazione: ne esiste infatti una versione per sistemi *Windows* e un'altra per *Linux* [4].

Infrastruttura

L'attacco è iniziato quando il gruppo criminale ha avuto accesso alla rete dell'oleodotto tramite un account VPN. Il primo giorno sono stati esfiltrati 100 GB di dati e il giorno successivo è avvenuta l'esecuzione che ha colpito molti sistemi informatici, inclusi quelli di amministrazione (fatturazione e contabilità) e di gestione.

I criminali hanno richiesto un riscatto di quasi 5 milioni di dollari che sono stati versati in criptovaluta già il giorno successivo. Una volta ricevuto il denaro, gli attaccanti hanno stranamente fornito lo strumento di decrittografia. In realtà, l'azienda è riuscita a recuperare i propri sistemi grazie a copie di backup precedentemente effettuate, dato che lo strumento fornito comportava tempi di recupero estremamente elevati [5].

Secondo il *Diamond,* ciò costituisce un'**infrastruttura di tipo I** poiché gli aggressori scovano la vulnerabilità e diffondono l'attacco.

Avversario

I criminali hanno utilizzato il paradigma *Ransomware-as-a-Service* (*RaaS*) in quanto, non solo hanno creato e gestito il malware e la sua esecuzione ma anche l'infrastruttura e i portafogli virtuali necessari al pagamento del riscatto. Inoltre, per potenziare l'attacco hanno collaborato con operatori esterni che si occupavano principalmente di mettere a disposizione risorse e capacità di calcolo.

Meta caratteristica socio-politica

La *Colonial Pipeline* fornisce e trasporta gas e carburanti ad usi civili, industriali e militari dal Texas fino a New York.

Meta caratteristica tecnologica

Come spesso accade le infrastrutture critiche non sono adeguatamente protette ai rischi cyber odierni. *Colonial Pipeline* è un gruppo nato in un'epoca precedente alla rivoluzione digitale e i sistemi informativi e di gestione non erano sufficientemente sicuri.

Riassumendo, l'esecuzione è schematizzata nei seguenti passaggi:

Evento	Ipotesi/attuale	Descrizione
1 (reconnaissance)	Attuale	L'attacco è iniziato a causa del furto delle credenziali di accesso alla rete VPN.
2 (reconnaissance)	Ipotesi	Probabilmente le credenziali sono state rubate a seguito di un attacco di *Phishing.*
3 (delivery)	Attuale	Il ransomware tramite la rete VPN accede alla rete informatica.
4 (exploitation)	Attuale	Il ransomware procede con la *privilege escalation* al fine di disattivare i sistemi di sicurezza presenti.
5 (installation)	Ipotesi	Il ransomware procede ad installarsi così da garantire il controllo remoto e avviare una sua esecuzione.
6 (C2)	Ipotesi	Come meccanismo di C2 i comandi sono stati inoltrati sotto rete TOR utilizzando il software di controllo *Cobalt Strike*.
7 (action)	Attuale	Il ransomware prima di tutto ha esfiltrato 100 GB di dati. In seguito, ha cifrato tutti i dati presenti nel datacenter.

Arco	Confidenza	And/Or	Ipotesi/Attuale	Fornisce
A	Media	And	Attuale	-
B	Media	And	Attuale	Fornisce informazioni sull'infrastruttura da attaccare.
C	Alta	And	Attuale	-
D	Alta	And	Attuale	-
E	Alta	And	Attuale	-
F	Alta	And	Attuale	-

Attacco Regione Lazio

Descrizione

Durante la notte tra sabato sera, 31 luglio 2021, e domenica mattina, 1° agosto, i sistemi informatici della regione Lazio hanno subito un attacco ransomware, causando specialmente il fermo del portale di prenotazioni delle vaccinazioni contro il *COVID-19*.

I sistemi sono stati spenti durante la risposta agli incidenti per consentire la verifica interna dopo l'attacco e per evitare ulteriori infezioni. Da alcune ricerche condotte si evince la presenza del *RansomEXX* (precedentemente noto come *Defray777*) di proprietà del gruppo di cyber-criminali *Sprite Spider*.

L'aggressione è iniziata a seguito del furto di credenziali di un dipendente di *LazioCrea* (la società che gestisce i sistemi informatici della Regione) che ha consentito agli aggressori di accedere alla *VPN* e distribuire il ransomware nel CED regionale.

Impatto

L'attacco ha causato più di un mese di interruzioni dei servizi coinvolti, dal sistema sanitario online per i cittadini ai registri dei dati delle farmacie e perfino di altri settori come quello urbanistico. Fortunatamente i dati sono stati recuperati da una copia di backup.

Applicazione del Diamond

Vittima

La vittima è il CED della Regione Lazio e i servizi risiedenti.

Capacità

Come i ransomware della tipologia *double-extortion*, anche quest'ultimo ha crittografato i dati presenti nell'infrastruttura e ha cancellato (ma non criptato) le copie di backup presenti nei repository del datacenter; infine, ha richiesto un riscatto in bitcoin che la Regione dichiara di non aver mai pagato.

Infrastruttura

Secondo le indagini l'attacco è iniziato a seguito del furto di credenziali appartenenti a un dipendente di *LazioCrea,* probabilmente a seguito di un attacco di *Phishing* condotto in precedenza verso quest'ultimo.

Ciò ha consentito agli attaccanti di accedere alla rete VPN del CED e installare così il ransomware all'interno del datacenter.

Secondo il *Diamond,* ciò costituisce un'**infrastruttura di tipo I** poiché gli aggressori scovano la vulnerabilità e diffondono l'attacco.

Avversario

Secondo le indagini l'avversario è il gruppo di cyber-criminali *Sprite Spider* con l'utilizzo del ransomware *RansomEXX* (precedentemente noto come *Defray777*) di loro proprietà.

Meta caratteristica socio-politica

Inizialmente si pensava erroneamente che l'attacco fosse stato ideato da parte di comitati *no-vax* a livello europeo, dato che il servizio più colpito è stato proprio quello delle prenotazioni delle vaccinazioni.

In realtà, come noto ai ricercatori di sicurezza, il gruppo di cyber-criminali *Sprite Spider* è tristemente noto per condurre attacchi potenti principalmente verso enti pubblici; quindi, si escluderebbe il movente precedentemente citato.

Riassumendo, l'esecuzione è schematizzata nei seguenti passaggi:

Evento	Ipotesi/attuale	Descrizione
1 (reconnaissance)	Attuale	L'attacco è iniziato a causa del furto di credenziali appartenenti a un dipendente.
2 (reconnaissance)	Ipotesi	Probabilmente le credenziali sono state rubate a seguito di un attacco di *Phishing.*
3 (delivery)	Attuale	Il ransomware tramite la rete VPN accede al datacenter.
4 (exploitation)	Attuale	Il ransomware procede con la *privilege escalation* al fine di disattivare i sistemi di sicurezza presenti.
5 (installation)	Ipotesi	Il ransomware procede ad installarsi così da garantire il C2 e avviare una sua esecuzione.
6 (C2)	Ipotesi	Il ransomware viene comandato dai cyber-criminali.
7 (action)	Attuale	Il ransomware prima di tutto esfiltra i dati presenti, così da poterli pubblicare nel *DarkWeb* e procede quindi a cifrare tutti i dati presenti nel datacenter. Infine, elimina le copie di backup dai repository.
8 (action)	Ipotesi	Il ransomware si muove lateralmente nella rete così scovare altre macchine e infettarle.

Arco	Confidenza	And/Or	Ipotesi/Attuale	Fornisce
A	Media	And	Attuale	-
B	Media	And	Attuale	Fornisce i dati di accesso alla rete del CED.
C	Alta	And	Attuale	-
D	Alta	And	Attuale	-
E	Alta	And	Attuale	-
F	Alta	And	Attuale	-
G	Alta	And	Attuale	-

Conti *cyberattack* al Sistema Sanitario Irlandese (*HSE*)

Descrizione

Il 13 marzo 2021 un dipendente dell'*HSE* ha aperto un'e-mail di *Phishing* contenente un allegato malevolo in formato *Excel*, il quale ha installato silenziosamente una backdoor sulla workstation (di seguito denominata "*Patient Zero*") dello stesso; nei due mesi successivi ciò ha consentito ai criminali di reperire informazioni circa l'organizzazione interna della rete informatica per poi sferrare l'attacco.

Di seguito la timeline dell'avvenimento:

- 31 marzo; i servizi di *IDS* hanno rilevato l'esecuzione di due strumenti software malevoli, risalenti alla gang del *Conti Ransomware*, sulla workstation *Patient Zero*; purtroppo, tale messaggio di alert è stato ignorato dal team *IT*.
- 7 maggio; l'attaccante ha compromesso per la prima volta i server dell'*HSE* coinvolgendo, nei cinque giorni successivi, un totale di sei ospedali.
- 10 maggio; uno degli ospedali ha rilevato attività insolite sul proprio controller di dominio *Microsoft Windows Server*; in seguito, il software antivirus dell'ospedale ha identificato il ransomware ma non è riuscito a metterlo in quarantena.
- 13 maggio; il provider di sicurezza antivirus dell'*HSE* ha inviato un'e-mail al team *IT*, evidenziando alcuni eventi critici non gestiti risalenti al 7 maggio su almeno 16 macchine [6].

Applicazione del Diamond Model

Vittima

Non solo è stato colpito il Sistema Sanitario Irlandese (*HSE*) ma si sono riversate gravi conseguenze anche per i servizi correlati, tra cui diversi pronto soccorso, assistenze sanitarie, ambulatori e farmacie. Il ransomware ha bloccato anche dati critici, tra cui cartelle cliniche elettroniche, prenotazioni delle sale operatorie e appuntamenti ambulatoriali [6].

Capacità

Il ransomware ha criptato circa l'80% dei dati presenti nel datacenter e sono stati esfiltrati circa 700 GB di dati, comprese le informazioni sanitarie sensibili (parte dei dati è stata successivamente rintracciata su un server commerciale degli *USA*) [6].

Infrastruttura

L’attacco è iniziato da un’e-mail di *Phishing* condotta verso un dipendente dell’*HSE* recapitata nella giornata del 13 marzo; essa conteneva un allegato malevolo in formato *Microsoft Excel* che ha installato una backdoor sulla workstation zero per poi procedere con l’attacco.

Secondo il *Diamond,* ciò costituisce un'**infrastruttura di tipo I** poiché gli aggressori scovano la vulnerabilità e diffondono l'attacco.

Avversario

Le indagini hanno provato che si tratta del *Conti Ransomware*, un malware di origine russa scritto in linguaggio C/C++ specializzato nel cifrare velocemente grandi quantità di file locali di una macchina.

Meta caratteristica socio-politica

L'Health Service Executive (*HSE*) irlandese è il sistema sanitario del Paese finanziato con fondi pubblici nell'ambito del Dipartimento della Salute, composto da 54 ospedali pubblici direttamente sotto l'autorità *HSE* e ospedali volontari che utilizzano l'infrastruttura *IT* nazionale.

È inestimabile il danno causato dal ransomware in quanto, oltre alla cifratura, i dati (specialmente quelli sensibili) sono stati diffusi pubblicamente. Inoltre, sono stati colpiti anche i servizi correlati al sistema sanitario nazionale, causando enormi disagi, anche di vitale importanza.

Meta caratteristica tecnologica

Come spesso accade in tali casi la causa principale è stata la mancanza di protezione e di attenzione; tra le varie debolezze della rete si evidenzia in particolare che:

- gli ospedali interessati utilizzavano decine di migliaia di sistemi operativi non solo obsoleti (principalmente Windows XP e Windows 7) ma anche non adeguatamente protetti;
- gli amministratori *IT* del sistema sanitario spesso ignoravano messaggi critici circa la sicurezza dei sistemi del datacenter e, di conseguenza, nelle fasi preliminari dell’attacco non sono riusciti a rispondere a molteplici segnali di avvertimento dell'imminente disastro.

Riassumendo, l’esecuzione è schematizzata nei seguenti passaggi:

Evento	Ipotesi/attuale	Descrizione
1 (reconnaissance)	Attuale	L'attacco è iniziato dall'apertura di un allegato malevolo all'interno di un'e-mail di *Phishing* sulla workstation di un dipendente.
2 (delivery)	Attuale	L'allegato ha installato una backdoor che ha consentito ai criminali di raccogliere informazioni circa la struttura interna della rete informatica.
3 (exploitation)	Attuale	Tramite la backdoor il ransomware ha raggiunto il datacenter.
4 (installation)	Attuale	Il ransomware è stato installato e avviato.
5 (C2)	Attuale	Il ransomware è stato controllato da remoto grazie alla backdoor basata su canali Tor e il software di controllo remoto Cobalt Strike [7].
6 (action)	Attuale	Il ransomware ha dapprima esfiltrato 700 GB di dati.
7 (action)	Attuale	Il ransomware ha cifrato circa l'80% del datacenter.

Arco	Confidenza	And/Or	Ipotesi/Attuale	Fornisce
A	Media	And	Attuale	-
B	Media	And	Attuale	Fornisce informazioni sull'infrastruttura da attaccare.
C	Alta	And	Attuale	-
D	Alta	And	Attuale	-
E	Alta	And	Attuale	-
F	Alta	And	Attuale	-

Conclusioni

Sintesi del documento con discussione dei risultati ottenuti e possibili sviluppi futuri.

Il documento ha ampiamente descritto sia dal lato teorico che pratico il *Diamond Model* of *Intrusion Analysis* e illustrato una sua applicazione a casi di *Ransomware* realmente accaduti.

Per ciascun episodio, partendo dall'analisi dell'evento di intrusione, sono state rilevate dapprima le sue caratteristiche principali (avversario, vittima, infrastruttura e capacità) per poi decorarlo con funzionalità secondarie che hanno consentito di mettere in relazione tutti gli aspetti dell'evento stesso. Quindi, dall'analisi, sono stati derivati alcuni approcci per fornire ai professionisti un modello che consenta di supportare efficacemente l'analisi e la prevenzione degli attacchi *Ransomware*.

Nel documento è stata riportata un'applicazione manuale del modello *Diamond sui* casi di studio citati. Un possibile sviluppo futuro potrebbe essere quello di automatizzare l'applicazione del modello mediante tool informatici e utilizzando l'intelligenza artificiale. Ad esempio, esso potrebbe essere integrato in alcuni strumenti analitici che ricevendo i dati da altri apparati informatici o da alcuni report forniti siano in grado di generare alcune ipotesi così da supportare gli analisti nel loro compito, migliorare il processo decisionale e puntare efficacemente sulla prevenzione degli attacchi.

Bibliografia

[1] «Kaspersky WannaCry,» [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. [Consultato il giorno 18 Luglio 2022].

[2] «WannaCry, dynamic malware analysis,» [Online]. Available: https://www.researchgate.net/publication/323202914_Demystifying_Ransomware_Attacks_Reverse_Engineering_and_Dynamic_Malware_Analysis_of_WannaCry_for_Network_and_Information_Security. [Consultato il giorno 17 Luglio 2022].

[3] «Diffusione di WannaCry,» [Online]. Available: https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/. [Consultato il giorno 17 Luglio 2022].

[4] «Colonial Pipeline,» [Online]. Available: https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/. [Consultato il giorno 07 Agosto 2022].

[5] «Colonial Pipeline attacco,» [Online]. Available: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know. [Consultato il giorno 07 Agosto 2022].

[6] «Conti Cyber on HSE,» [Online]. Available: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf. [Consultato il giorno 07 08 2022].

[7] «Conti HSE C2,» [Online]. Available: https://heimdalsecurity.com/blog/what-is-conti-ransomware/. [Consultato il giorno 07 08 2022].