UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

"Cybersecurity e protezione degli endpoint. Analisi comportamentale Trojan con Crowdstrike"

Relatore: Prof. / Dott Bresolin Davide

Laureando: Tommaso Peruzzo

ANNO ACCADEMICO 2022 – 2023

Data di laurea 18/07/2023

INDICE

Introduzione

La sicurezza informatica risulta essere uno tra gli elementi che non possono essere più trascurati dalle aziende. Un possibile attacco informatico può infatti provocare danni sotto vari aspetti: da quello economico dovuto alla sospensione dei servizi aziendali ed al ripristino degli stessi, a quelli reputazionali dovuti alla perdita di fiducia da parte dei propri clienti.

Lo scopo dell'elaborato è quello di far comprendere al lettore l'importanza che la sicurezza informatica ha al giorno d'oggi, illustrando i pericoli da cui essa protegge, gli strumenti che possono essere utilizzati per facilitarne l'implementazione e l'attività di studio di un malware che può essere svolta da team di analisti di cybersecurity.

Nel primo capitolo vengono introdotti dei concetti alla base del trattamento dei dati sensibili, spesso obiettivo degli attacchi informatici. Alcuni tra gli attacchi più di rilievo a livello mondiale degli ultimi anni vengono riepilogati ed analizzati, con un resoconto degli impatti economici da essi causati. Anche il panorama italiano risulta essere spesso bersaglio di gruppi di cybercriminali e, nonostante i recenti investimenti, i danni restano comunque ingenti.

A difesa delle reti aziendali, possono essere impiegati diversi tipi di strumenti. Nel secondo capitolo vengono illustrati e spiegati alcuni di essi che vengono utilizzati dagli analisti di cybersecurity per monitorare le attività all'interno delle reti aziendali. Tra questi vi sono i SIEM, gli EDR e XDR, tecnologie approfondite singolarmente per evidenziare pregi e difetti di ciascuna di esse.

Nel terzo capitolo, un approfondimento del mondo degli EDR, con particolari riferimenti all'EDR Crowdstrike[1], di cui vengono elencate le sue funzionalità, l'approccio che lo strumento utilizza per garantire la sicurezza degli endpoint, come deve essere installato ed inserito all'interno delle aziende, alcuni dei suoi moduli e la differenza tra rilevamento e prevenzione da esso applicata.

I malware Trojan sono stati da sempre un veicolo di infezione largamente utilizzato, grazie alle loro capacità di camuffamento in processi leciti e quindi non rilevabili agli occhi di utenti inesperti. Nel quarto capitolo si possono evincere dei loro tratti caratteristici.

[1] https://www.crowdstrike.com/it/

Viene approfondito il Trojan Andromeda, come è stato responsabile della creazione di una delle botnet più longeve dell'ultimo decennio e come, grazie all'utilizzo di strumenti come Crowdstrike, malware di questa tipologia possono essere riconosciuti, rilevati ed arrestati all'interno di macchine impattate.

L'analisi del malware è stata da me svolta durante il mio tirocinio curricolare che ho effettuato presso l'azienda di cybersecurity HWG Srl[2]. Un aspetto importante sulla quale la tesi si basa, infatti, è dovuto a questa esperienza durante la quale ho potuto apprendere ed approfondire nozioni utili alla stesura dell'elaborato.

Il tirocinio mi ha permesso di essere inserito all'interno di un SOC e di essere affiancato nel mio percorso di formazione, per accrescere le mie conoscenze nell'ambito della cybersecurity. Ho potuto utilizzare strumenti quali i SIEM di Qradar e Splunk, EDR come Crowdstrike o Microsoft Defender, XDR di Taegis o Exabeam ed altre piattaforme grazie alle quali gli analisti di cybersecurity monitorano e difendono quotidianamente le reti aziendali a livello globale. Tramite queste tecnologie, infatti, i SOC ricevono segnalazioni di anomalie all'interno delle reti e dovranno gestirle con le dovute analisi del caso, creando un report dell'attività rilevata da inviare ai propri clienti.

Questi aspetti saranno dei suoi punti cardine e materiale per le considerazioni nel capitolo conclusivo. In esso, viene fatta un'ultima considerazione personale sugli aspetti analizzati nei capitoli precedenti, unendo i concetti di cybersecurity introdotti e l'importanza che il tirocinio ha avuto nel mio percorso accademico.

[2] https://www.hwg.it/

CAPITOLO 1: CYBERSECURITY AZIENDALE

La sicurezza informatica è un aspetto di fondamentale importanza per le aziende che intendono proteggere sé stesse e, indirettamente, i dati sensibili dei propri dipendenti e clienti.

Gli attacchi informatici non avvengono per una dimostrazione di abilità da parte dei cyber criminali. I loro reali bersagli sono i dati sensibili, in quanto la loro rivendita può portare ampli profitti.

I dati personali includono nomi, dettagli genetici, biometrici o inerenti alla salute, informazioni del web come indirizzi IP, indirizzi e-mail personali, opinioni politiche e orientamento sessuale; al contrario, i dati non personali possono includere numeri di registrazione delle società, indirizzi di posta elettronica generici (es. info@azienda.com) e dati resi anonimi.

Il 25 maggio 2018 è stato introdotto il GDPR, Regolamento Ue 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali[3].

Seppur l'introduzione del GDPR abbia obbligato le aziende ad adattarsi a standard più rigidi e con conseguenti costi di implementazione, allo stesso tempo ha portato loro diversi benefici, in quanto si sono viste obbligate a razionalizzare i processi e procedure, dovendone curare maggiormente gli aspetti della gestione dei dati e della sicurezza nella globalità. Tutto ciò ha portato ad un cambio di mentalità nell'ottica di avere una maggiore protezione dei dati e chi è riuscito ad applicare questi nuovi processi in tempi brevi, ha potuto ottenere una maggior fiducia da parte dei propri clienti.

I dati dell'azienda e dei clienti, infatti, rappresentano il cuore di ogni business e come tali sono considerati il bersaglio di cyber attacchi: un'azienda che riesce a tutelare i propri dati e quelli dei suoi clienti, fa sentire questi ultimi al sicuro e incentivati ad utilizzare i propri servizi.

Ciononostante, si cercano spesso compromessi per ridurre le spese derivanti dalla corretta gestione e applicazione di questo regolamento, come affidarsi a strutture non sufficientemente qualificate per effettuare questo tipo di lavori. Queste scelte si trasformano per le aziende in possibili pericoli, lasciando aperte falle nei sistemi che, puntualmente, i gruppi di cybercriminali riescono a sfruttare creando non pochi disagi.

[3] https://neinformatica.it/blog/privacy-e-sicurezza/gdpr-unopportunita-per-le-aziende/

1.1. Panoramica Incidenti e costi per le imprese

Gli ultimi 4 anni si sono rivelati i peggiori di sempre in termini di evoluzione degli attacchi informatici, sia numericamente che per impatto, con un trend in persistente crescita delle loro gravità e conseguenti danni[4].

I nuovi metodi di comunicazione digitale, lo shopping online, il lavoro da remoto ed altri fattori hanno contribuito ad aumentare il numero di dati personali sensibili reperibili nella rete.

Questa ondata di digitalizzazione ha portato gli hacker ad avere a disposizione sempre più bersagli tra le crescenti reti aziendali, grazie alla presenza di possibili maggiori punti di accesso. Di conseguenza, ha acquisito una notevole importanza per le aziende l'identity protection, ovvero la gestione delle identità e delle utenze lavorative; l'assicurarsi che ogni attività proveniente da un endpoint sia autentica, come anche che l'utenza stessa sia effettivamente utilizzata dalla persona corretta.

L'MFA (Multi Factor Authentication) gioca un ruolo chiave come garanzia per tutte queste attività. L'inserimento di un ulteriore codice, recapitabile solamente in un dispositivo dell'utente che sta cercando di effettuare l'attività di login, permette di avere una maggiore sicurezza sulla reale identità dello stesso.

Nonostante questi metodi di sicurezza aggiuntivi, non tutte le aziende si sono attrezzate tempestivamente, aprendo così la strada ai gruppi di cybercriminali. In quell'anno, infatti, essi si sono focalizzati sullo sviluppo ed evoluzione del codice base di trojan bancari, al fine di evitare le preesistenti misure di sicurezza di cui le compagnie erano dotate.

È questo il caso del Trojan ZeuS, uno dei più famosi trojan[5] dal 2007, primo anno in cui venne utilizzato per rubare dati all'United States Department of Transportation. Nel corso dei due successivi anni, si stima che ZeuS abbia infettato 3.6 milioni di PC negli Stati Uniti, fino allo stop delle sue attività nel 2010, quando intervenne anche l'FBI, arrestando oltre 100 persone coinvolte per i loro furti, che portarono ad un ammontare di 70 milioni di dollari rubati.[6]

Dopo aver infettato la macchina, ZeuS ne monitorava l'utilizzo, copiando i dati utili agli attaccanti ed inviandoli ad un bot server di comando e controllo (C2C). Questo malware veniva venduto come toolkit[7] per l'installazione di diversi suoi moduli, quali "Backconnect" (1500$) o "Firefox form

[4] https://finanza.lastampa.it/News/2023/02/07/cybersecurity-+53percento-di-attacchi-informatici-negli-ultimi-4-anni/OTlfMjAyMy0wMi0wN19UTEI

[5] Tipologia di malware che si maschera dietro applicativi apparentemente leciti.

[6] https://en.wikipedia.org/wiki/Zeus_(malware)

[7] Insieme di strumenti e software (spesso librerie), utilizzati per facilitare l'utilizzo e sviluppo di applicazone più complesse (https://it.wikipedia.org/wiki/Toolkit)

grabber" (2000$). Il primo permetteva la connessione da remoto ai computer infetti e simulare pagamenti da essi, il secondo di estrarre credenziali inserite nel browser di Firefox, al fine di poterle rivendere (Fig.1).[8]

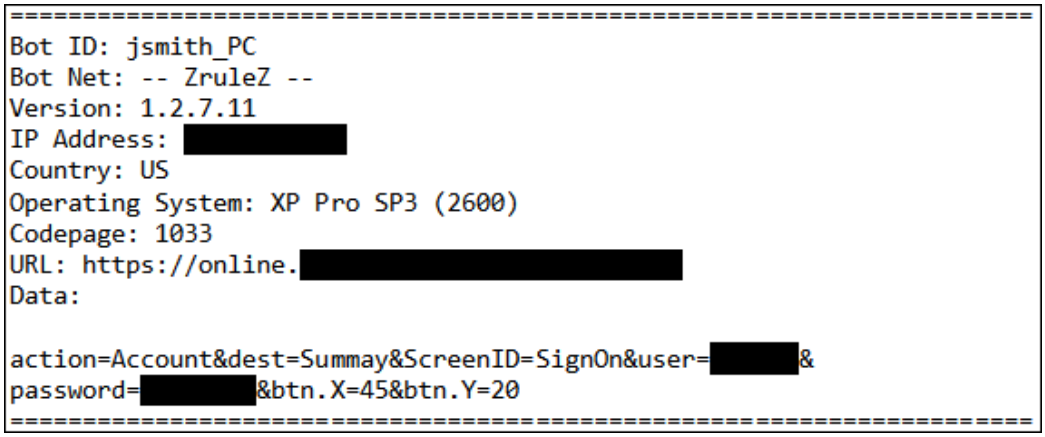

Figura 1 - Esempio di informazioni bancarie ottenute da un sistema infettato da ZeuS. FONTE: https://www.secureworks.com/research/zeus

ZeuS continuò a ricevere modifiche negli anni, fino ad arrivare al 2019, anno in cui trojan più moderni hanno iniziato a sfruttare le sue tecniche di injection[9], facendosi largo nel panorama globale dei cybercrimini. TrickBot è il primo di essi in quell'anno[10].

Lo scopo primario di queste nuove minacce non era quello di limitarsi alle sole banche, ma, con l'adozione di nuovi approcci e tecniche, anche ad altri settori, come quelli industriali. L'inserimento di questi nuovi settori bersaglio era principalmente dovuto ad una nuova pericolosa minaccia che iniziava a prendere sempre più piede: il ransomware.

Questa tipologia di malware è studiata per criptare files nei dispositivi ed espandersi poi ad altri collegati all'interno della stessa rete, bloccando così l'operatività di vari sistemi o intere aziende.

Subentra poi il meccanismo della quadrupla estorsione, ossia la richiesta di un riscatto per evitare quattro possibili minacce o problematiche, che emergono nel momento in cui un ransomware ha agito all'interno di una compagnia. Le vittime inizialmente ricevono la richiesta di pagamento per poter decriptare i propri dati e ritornare in possesso delle loro informazioni. Allo stesso modo, ciò permetterebbe anche di ovviare al secondo problema, ossia quello di riuscire a tornare operativi ed assicurare una continuità dei propri servizi. Il terzo aspetto consiste nel recupero dei propri dati sensibili al fine di evitarne la diffusione nel dark web, attività che potrebbe andare ad avvantaggiare

[8] https://www.secureworks.com/research/zeus
[9] "Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges." (https://attack.mitre.org/techniques/T1055/)
[10] X-Force Threat Intelligence Index Produced by IBM X-Force Incident Response and Intelligence Services (IRIS) 2020

le aziende concorrenti, nonché causare una perdita di immagine da parte dell'azienda stessa. Il recupero dei dati vanificherebbe anche la quarta minaccia: l'utilizzo delle proprie informazioni per contattare clienti e partner, estendendo la pericolosità del ransomware e danneggiando, ancora una volta, la reputazione aziendale.

Il 2020 è stato l'anno caratterizzato da un notevole incremento di questa tipologia di malware. Il 23% di tutti gli attacchi informatici, infatti, è stato ricondotto ai ransomware, con un incremento del 160% di furti di dati ad essi collegati, rispetto al 2019. Complice di questo dilagamento è stato l'incremento dell'efficacia delle campagne di phishing. In quell'anno esse hanno rappresentato il 33% dei vettori di attacco iniziale, portando alcuni applicativi, primo fra tutti Emotet, a raggiungere il loro apice di infettività. Emotet è un framework molto conosciuto nel Dark Web, dove viene largamente acquistato grazie alle sue funzioni in continua evoluzione e ai conseguenti miglioramenti.[11] Utilizzato per le prime volte nel 2014 come banking trojan, si è evoluto nel tempo con nuovi moduli, come quello di spam bot o di DDoS[12], fino ad arrivare a più moderne strutture anti-analisi, per evitarne la rilevazione da parte degli antivirus. Quest'ultime sono state implementate tramite un packer scritto ad-hoc per renderne la decompilazione più complessa o sistemi di "VM-detection" e per riuscire ad individuare la tipologia di ambiente nel quale esso si sta eseguendo, reale o artificiale come in una Virtual Machine.

Una costante nel suo funzionamento è però il metodo di divulgazione: un recapito alle vittime di un messaggio di posta elettronica con un file allegato, tipicamente appartenente al mondo Office. Questi file contengono macro che, una volta aperti, eseguon o codice all'interno delle macchine, avviando così l'infezione tramite tattiche di Persistence (secondo il "Mitre Att&ck": "tecniche che gli avversari utilizzano per mantenere l'accesso ai sistemi anche dopo i riavvii, la modifica delle credenziali e altre interruzioni che potrebbero interrompere l'accesso")[13].

Le attività collegate a ransomware sono state molteplici nel 2020, come quella che nel mese di giugno ha colpito la multinazionale energetica italiana "Enel Group" (Fig.2), vittima della cybergang Netwalker, la quale riuscì a violare la rete interna dell'azienda tramite l'utilizzo del ransomware Snake, noto anche come EKANS. La stessa ha chiesto un riscatto di 14 milioni di dollari per la chiave

[11] https://www.cybersecurity360.it/nuove-minacce/emotet-il-piu-pericoloso-framework-criminale-di-cyber-spionaggio-storia-evoluzione-e-tecniche-di-attacco/

[12] "Con l'acronimo DoS (Denial-of-Service) si indica comunemente una famiglia di attacchi informatici orientati a colpire la disponibilità di uno o più servizi inibendone l'accesso; nel caso in cui questo tipo di attacco venga eseguito mediante l'utilizzo di sorgenti multiple distribuite viene identificato come Distributed Denial of Service, abbreviato con l'acronimo DDoS." (https://www.csirt.gov.it/contenuti/attacchi-ddos-tipologie-e-azioni-di-mitigazione)

[13] Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code. (https://attack.mitre.org/tactics/TA0003/)

di decrittazione e per evitare il rilascio di 5 TB di dati rubati. Non sono state divulgate informazioni circa il pagamento del riscatto da parte dell'azienda, ma a novembre, in un forum del deep web, era possibile trovare il data leak in vendita per 1000$.[14]

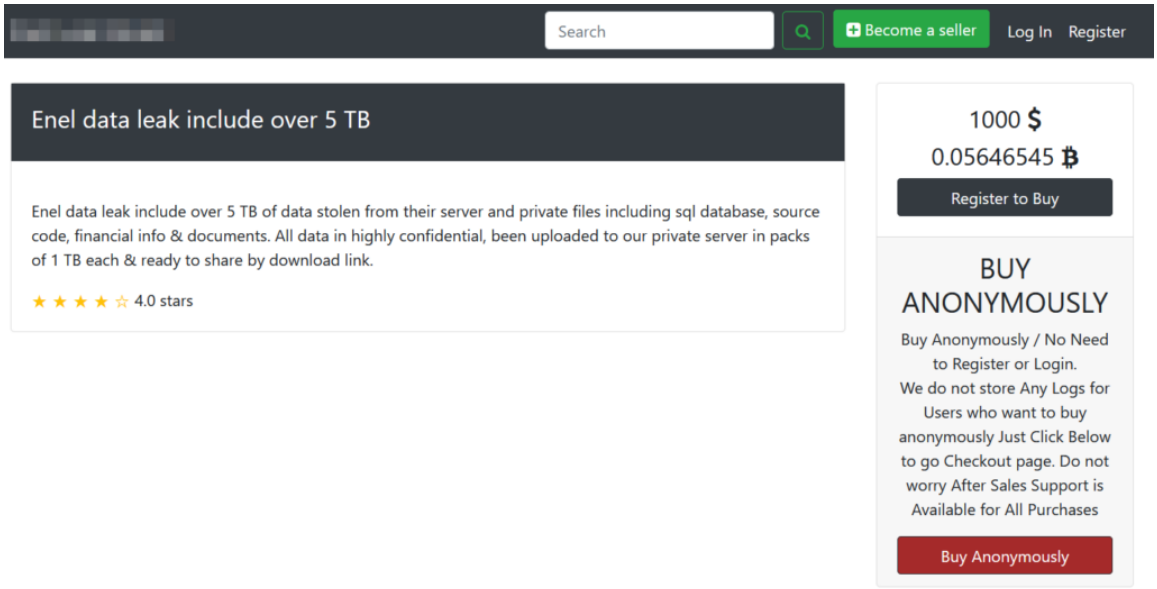

Figura 2 - Dati Enel in vendita in un noto market underground. FONTE: https://www.redhotcyber.com/post/rhc-rileva-4tb-di-dati-di-enel-in-vendita-nelle-underground-per-1000-euro-si-tratta-dellattacco-di-netwalker/

Seppur le organizzazioni cybercriminali professino una certa "correttezza etica" e l'intento di non arrecare danni a servizi sanitari, i cyber attacchi verso questi ultimi sono aumentati del +47% nel 2020, rispetto al precedente anno.

È il caso di Wizard Spider, un gruppo di criminali informatici di San Pietroburgo, che ha realizzato a maggio 2020 un attacco informatico contro il servizio sanitario nazionale irlandese, sfruttando un ransomware chiamato "Conti".

La richiesta di riscatto ha ammontato a 14 milioni di sterline (circa 17 milioni di euro). In questo caso però, le autorità irlandesi non sono scese a patti, portando alla creazione di situazioni di disagio per i pazienti, in quanto la banda criminale ha focalizzato le attività nella divulgazione di informazioni riservate di circa 520 persone e nella modifica dei loro appuntamenti, obbligando il sistema all'abbandono del digitale per mesi. Questa coraggiosa scelta, ha però causato allo stato una perdita economica di circa 100 milioni di euro.[15]

Ogni anno Palo Alto Networks stila un report sull'andamento delle attività del mondo del cybercrimine. Nel 2020, è stato calcolato che la richiesta di riscatto più alta sia stata di 30 milioni di dollari mentre il gruppo di ransomware più attivo è stato Sodinokibi (noto anche come REvil).

[14] https://www.redhotcyber.com/post/rhc-rileva-4tb-di-dati-di-enel-in-vendita-nelle-underground-per-1000-euro-si-tratta-dellattacco-di-netwalker/
[15] https://www.openpolis.it/durante-la-pandemia-aumentano-gli-attacchi-informatici-in-ue/

Quest'ultimo è responsabile del 22% di tutti i ransomware osservati da X-Force in quell'anno. Da una stima fatta da IBM, risulta che abbia esfiltrato circa 21,6 terabyte di dati e che quasi due terzi delle vittime abbiano pagato il riscatto richiesto, mentre circa il 43% ha perso i propri dati. Il risultato è che i responsabili di Sodinokibi hanno guadagnato oltre 123 milioni di dollari in un solo anno.[16]

Lo stesso trend ha continuato ad anche neli nel 2021 (Fig.3). Le infezioni da ransomware hanno comportato una richiesta di riscatto media pari a circa 5,3 milioni di dollari, il 518% in più rispetto al 2020. Allo stesso tempo, non tutte le richieste vengono soddisfatte, ma il pagamento medio effettuato resta comunque un campanello di allarme importante, ad evidenziare un problema in continua crescita: 570mila dollari con un +82% rispetto al 2020.[17]

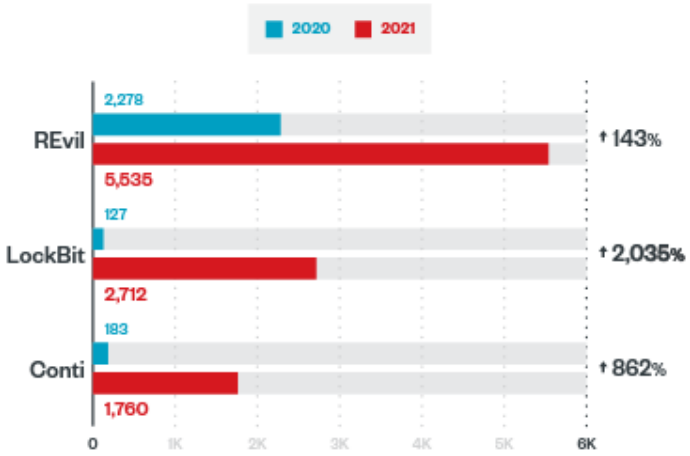

Figura 3 - Andamento famiglie Ransomware nel 2020 e 2021. FONTE: https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

Nel 2021, uno dei più noti attacchi è stato sferrato verso la software house Kaseya. La società fornisce sistemi di monitoraggio della rete ad aziende terze e il malware si è potuto diramare così a 54 dei suoi clienti. Per il rilascio dei dati criptati a tutte le aziende coinvolte, REvil ha fatto una richiesta complessiva di 70 milioni di dollari, ridimensionata successivamente a 50. Questa cifra record è stata dovuta anche alla tipologia di servizi infettati, tra i quali la grande catena di supermercati "Coop", che si è vista costretta a chiudere circa 700 negozi. Una chiusura durata circa una settimana che potrebbe esser costata loro milioni di dollari.[18]

Un fenomeno in particolare espansione in quell'anno è stato quello del "RaaS" (Ransomware as a Service). RaaS è un acronimo utilizzato per definire dei tipi di ransomware che vengono venduti da gruppi di cybercriminali ad utenti o gruppi terzi. Questo tipo di vendita può essere fatto sotto forma di canone mensile o in percentuale del futuro guadagno ricavato dal suo utilizzo. Questa tipologia di

[16] https://www.cert.hu/sites/default/files/xforce_threat_intelligence_index_2021_90037390usen.pdf
[17] https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/
[18] https://www.cybersecurity360.it/nuove-minacce/ransomware/mega-attacco-ransomware-mondiale-via-kaseya-perche-e-allarme-rosso/

ransomware è diventata particolarmente pericolosa in quanto permette anche ad utenti meno esperti di entrare in possesso di materiali già pronti all'uso (tra i quali ransomware preimpacchettati, server C2C a disposizione, portali per la riscossione dei riscatti e dove pubblicare eventuali data leak) e di servizi di supporto 24/7, che li stimolano al loro utilizzo con più leggerezza, senza pensare alle possibili ripercussioni delle loro azioni. Fortunatamente, non tutti gli attacchi vanno a buon fine ma un'iscrizione mensile, che varia dai 40$ alle migliaia, contribuisce alla crescita dei gruppi ransomware ed al fenomeno dei RaaS, che solo nel 2021 ha generato una domanda di 6 milioni di dollari.[19] Uno dei maggiori esponenti tra i gruppi distributori di RaaS è LockBit.

Non a caso, il secondo attacco eclatante di quell'anno è stato quello nei confronti di Accenture, multinazionale da 60 miliardi di dollari di fatturato, operante nel settore dei servizi IT e di consulenza per gli stessi.[20] Il gruppo LockBit ha affermato di aver sottratto alle reti di Accenture un totale di 6 TB di dati ed ha chiesto all'azienda un riscatto di 50 milioni di dollari.[21]

Il 2021 è stato un anno di continua espansione del cybercrimine anche per l'Italia, partendo con l'attacco alla regione Lazio ad agosto. In quell'occasione l'attività è stata associata al malware RansomExx, che aveva già precedentemente colpito altri enti governativi del Brasile e Texas. Non sono state divulgate richieste di riscatto a riguardo ma è stata comunque rilevata la crittazione dei dati presenti su alcune virtual machine, tra cui degli applicativi che hanno causato il down di alcuni siti e piattaforme, e dei documenti regionali.[22]

Dopo questa prima fase, il 12 settembre l'Azienda Ospedaliera San Giovanni Addolorata ha appreso di essere stata vittima di un attacco informatico[23]: 300 server e 1500 client sono stati bloccati, rendendo irraggiungibili email e l'accesso alle cartelle cliniche o ai referti. Ciò ha obbligato l'ospedale a dover rifare un "tuffo nel passato" e per garantire il servizio si è dovuto procedere manualmente con carta e penna, senza alcuni sistemi informatici.

Nel panorama globale, la Russia si è dimostrata essere stata da sempre uno dei Paesi con più attori che contribuiscono alla crescita del mondo del cybercrimine.[24] Molti dei gruppi più famosi sono russi (REvil, Cozy Bear, Killnet), in diversi codici di ransomware sono stati trovati pezzi di testo russo e la maggior parte degli obiettivi di questi malware non sono Paesi facenti parte della CIS[25].

[19] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
[20] https://it.wikipedia.org/wiki/Accenture
[21] https://www.redhotcyber.com/post/accenture-timeline-dell-incidente-ransomware-lockbit-2-0/
[22] https://www.cybersecurity360.it/nuove-minacce/regione-lazio-vaccini-bloccati-poco-pronta-contro-il-ranwomare-ecco-perche/
[23] https://www.redhotcyber.com/post/san-giovanni-addolorata-di-roma-la-timeline-dell-attacco-ransomware/
[24] https://www.openpolis.it/durante-la-pandemia-aumentano-gli-attacchi-informatici-in-ue/
[25] "Comunità degli Stati Indipendenti" composta da 9 delle 15 ex repubbliche sovietiche. (https://it.wikipedia.org/wiki/Comunit%C3%A0_degli_Stati_Indipendenti)

Con la più recente guerra tra Russia ed Ucraina del 2022, poi, il problema non ha potuto fare altro che aggravarsi ulteriormente. In più situazioni, nel momento in cui qualcuno abbia manifestato sostegno per l'Ucraina o accusato la Russia, si sono successivamente presentati attacchi malevoli nei confronti degli stessi. È il caso del Parlamento europeo, il cui sito è stato bersagliato da un attacco DDos che ne ha compromesso la disponibilità. Il fatto è accaduto a novembre, dopo che l'ente "ha proclamato la Russia come Stato sponsor del terrorismo", in una risoluzione approvata a larga maggioranza.[26]

Questa tipologia di attacco è stata poi largamente riproposta dai cyber attori russi, provocandone un incremento del 258% nel 2022.

Una loro vittima è stata anche l'Italia che, a maggio di quell'anno, si è vista come bersaglio di attacci DDos vari siti di enti pubblici (tra cui ministero della Difesa, degli Esteri, il sito del Senato, quello della Corte dei Conti), elencati in un messaggio del gruppo Telegram di Killnet.
In quel caso, i danni non sono stati rilevanti ma l'obiettivo principale era quello di creare "rumore", colpendo infrastrutture pubbliche dall'alta rilevanza mediatica.

[26] https://www.ansa.it/europa/notizie/europarlamento/news/2022/11/23/cyberattacco-al-sito-del-parlamento-europeo-servizi-compromessi_961b642b-4dfa-4971-b8b6-8741ec375b11.html

1.2. Investimenti nel panorama italiano

Come evidenziato nel capitolo precedente, una carenza di attenzione verso gli aspetti della cybersecurity può comportare ingenti costi alle imprese.

Dopo l'introduzione del GDPR nel 2018 e con il trend in crescita dei cyber attacchi, anche il panorama italiano ha voluto adattarsi a questi nuovi fattori, aumentando gli investimenti nel campo della sicurezza informatica (Grafico 1).

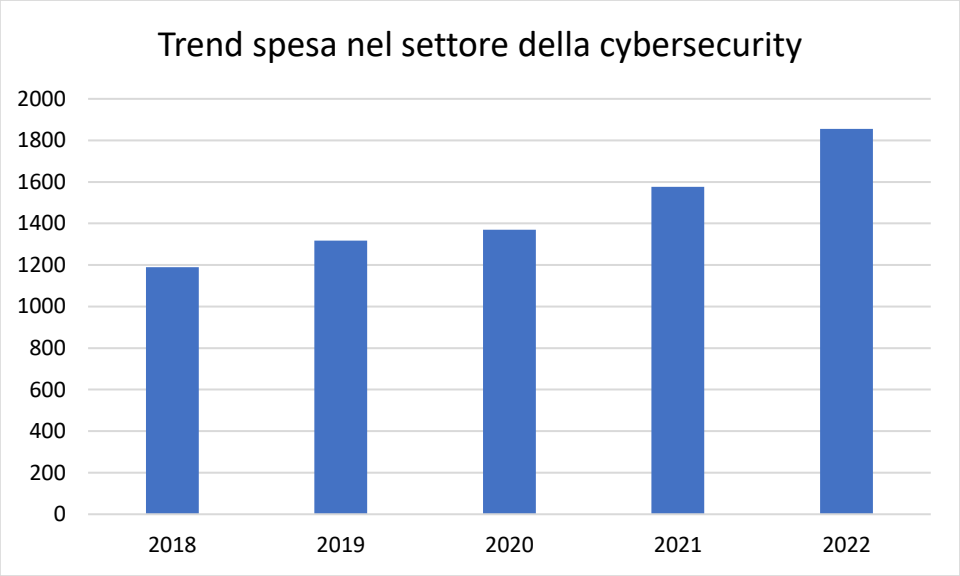

Grafico 1 - Elaborazione personale degli iInvestimenti in Italia. Dati in milioni di euro.

Lo scorso anno sono stati raggiunti gli 1.855 milioni di euro, il 18% in più rispetto al 2021. Nonostante ciò però, l'Italia è all'ultimo posto dei Paesi del G7 in termini di rapporto tra investimenti nella cybersecurity e PIL(0,10%), dove invece spiccano USA e UK (0,31%) con un rapporto che triplica quello italiano.[27] Da anni questo trend italiano è in calo e sembra che di ciò ne siano a conoscenza anche i cyber criminali perché implica che gli investimenti fatti non sono sufficienti, senza contare il fatto che si dovrebbe approfondire il modo in cui questi vengono spesi.

Col PNRR (Piano Nazionale di Ripresa e Resilienza) sono stati stanziati fondi per migliorare le soluzioni tech del Paese pari a 623 milioni di euro, in gestione all'Agenzia per la Cybersicurezza Nazionale (ACN). Questo ente è stato istituito dopo l'incursione degli hacker nei sistemi della regione Lazio, attività documentata nel capitolo precedente.[28]

[27] https://www.ilsole24ore.com/art/cybersecurity-mercato-balza-19-miliardi-italia-AEiqjkrC (Politecnico di Milano)
[28] https://www.cybersecurity360.it/outlook/pnrr-e-cyber-security-la-vera-sfida-e-investire-meglio/

Nonostante gli investimenti però, gli enti governativi italiani hanno subito 9% degli attacchi derivanti da vulnerabilità dei sistemi non patchate (Grafico 2), lasciando spazio agli attaccanti di sfruttarle per diversi tipi di infiltrazione nei sistemi.

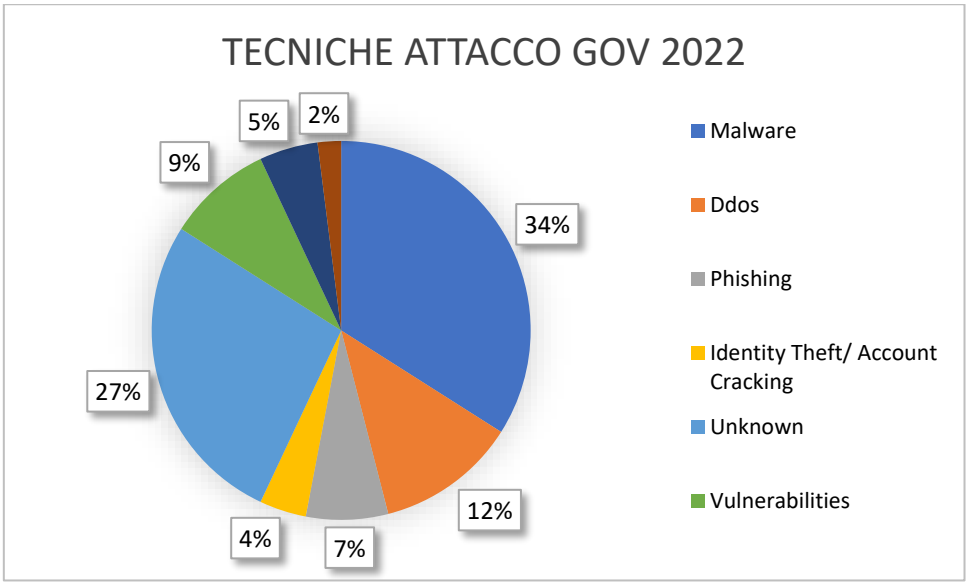

Grafico 2 - Elaborazione personale delle tecniche di attacco verso enti governativi nel 2022

Queste mancanze di accortezze e di sensibilizzazione, nonché formazione, del personale (7% degli attacchi derivanti da phishing) hanno contribuiti negli ultimi anni a rendere l'Italia uno dei Paesi maggiormente colpiti (Grafico 3).

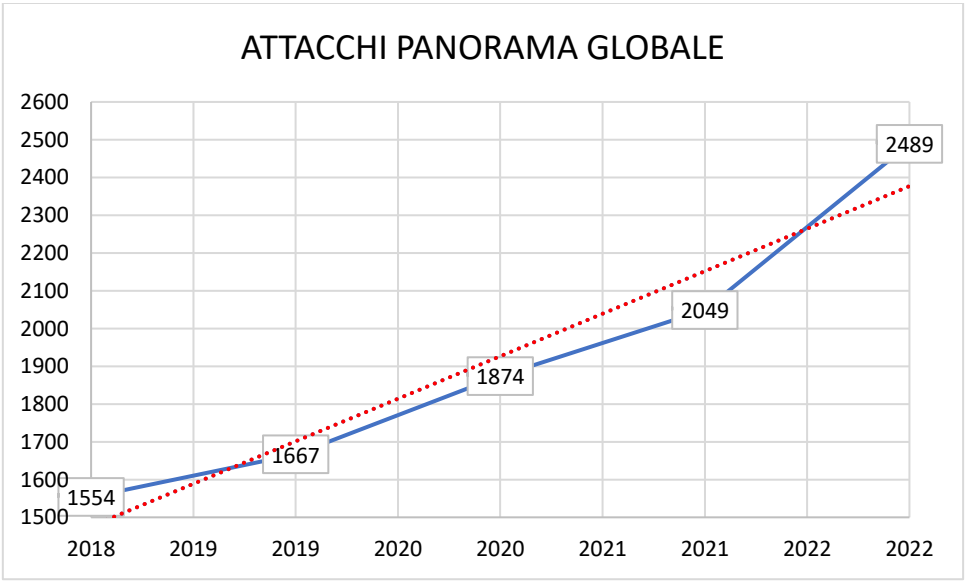

Grafico 3 - Elaborazione personale degli attacchi mondiali negli anni 2018-2022

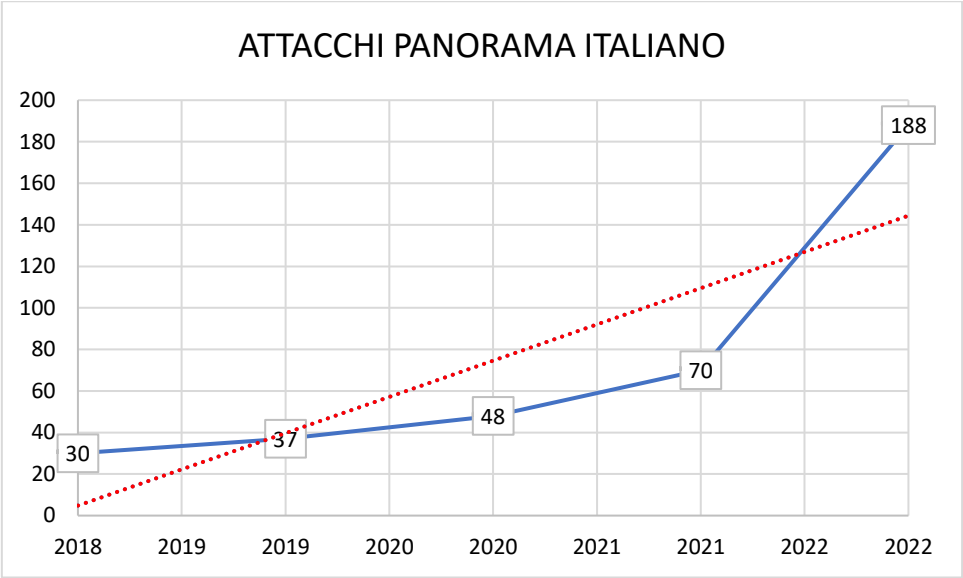

Grafico 4 - Elaborazione personale degli attacchi italiani negli anni 2018-2022

Come a livello globale, anche per l'Italia gli attacchi hanno registrato picchi sempre più alti (Grafico 4 e Grafico 5), ma ciò che dovrebbe preoccupare maggiormente è la crescita percentuale rispetto al panorama globale, che ha portato l'Italia a rappresentare il bersaglio del 7,6% degli attacchi mondiali.[29]

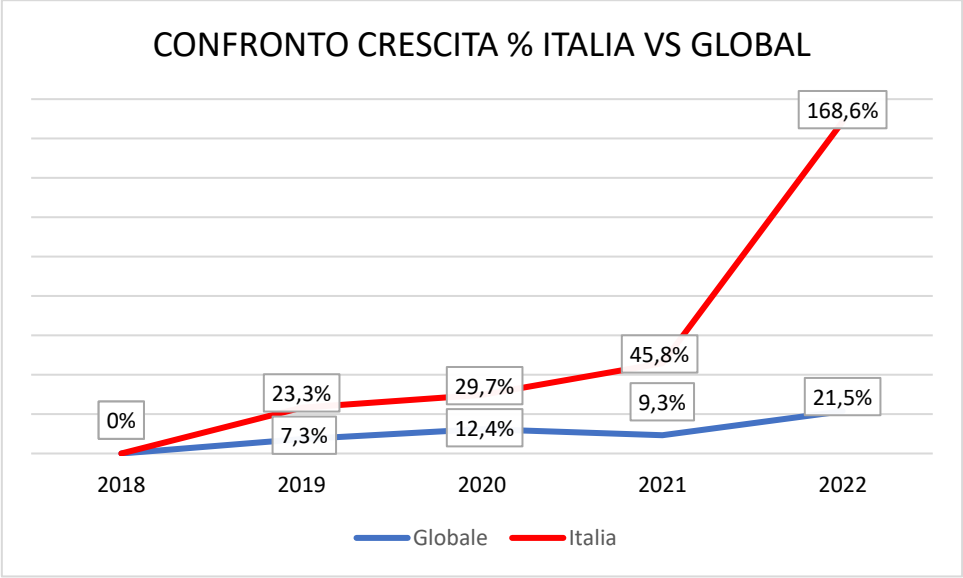

Grafico 5 - Elaborazione personale del confronto di crescita percentuale dal 2018 al 2022

Considerando che l'Italia rappresenta il 2,2% del PIL globale e lo 0,75% della popolazione globale, i dati riportati dai precedenti grafici sono numeri che dovrebbero allarmare.

[29] Rapporto Clusit 2023: https://clusit.it/rapporto-clusit/

CAPITOLO 2: SOLUZIONI

Per ridurre le minacce derivanti dal mondo cybercrimine e permettere alle aziende di mantenere il controllo dello stato di salute dei propri sistemi esistono diverse tecnologie.
Queste soluzioni vanno scelte in base alle diverse esigenze, tipologia di attività da monitorare ed anche alle soluzioni già presenti in una rete aziendale.
Durante il mio periodo di tirocinio, ho potuto lavorare all'interno di un SOC (Security Operation Center), che ha lo scopo di monitorare, attraverso diversi tipi di strumenti di gestione e sicurezza, l'attività delle reti aziendali dei vari clienti e segnalar loro qualsiasi anomalia o comportamento sospetto che vengano riscontrati.
Le 3 soluzioni che ho potuto utilizzare durante tale periodo e che verranno introdotte nei prossimi paragrafi sono: SIEM, EDR, XDR.

2.1. SIEM

Un SIEM (security information and event management) è uno strumento volto alla raccolta centralizzata ed elaborazione dei log all'interno di una rete.

Nasce nel 1997 dall'unione di SIM (Security Information Management) e SEM (Security Event Mangament), due soluzioni simili ma con scopi diversi, al fine di ridurre i falsi positivi generati dai NIDS (Network Intrusion Detection System).[30] Il primo, è un sistema che automatizza il processo di raccolta dei log tramite l'installazione di un software agent su vari tipi di dispositivi aziendali, con il compito di inviarli a server centralizzati, dove vengono elaborati e standardizzati.
Il SEM è una soluzione che, a differenza della prima, opera in tempo reale e gestisce gli eventi, monitorandoli, correlandoli e creando risposte automatiche a determinate situazioni.

Unendo i due strumenti si ottiene il funzionamento del SIEM: un log, generato da specifiche apparecchiature ove installato un agent apposito (ad esempio firewall, IDS[31], DNS server, dispositivi utenti, VPN), viene inviato ad un server dove viene raccolto e salvato per poi essere standardizzato, creando così un evento. Gli eventi vengono elaborati tra di loro e nel momento in cui una correlazione degli stessi comporti la rilevazione di un comportamento sospetto/errato, viene generata una segnalazione che dovrà essere gestita dall'uomo, il cui compito sarà quello di risolvere l'anomalia riscontrata all'interno della rete in esame.

Nel tempo il SIEM si è evoluto come strumento, fino ad arrivare alla quarta generazione nel 2017, nella quale sono state integrate le prime tecniche basate sull'IA (in particolare il Machine Learning),

[30] https://www.cybersecurity360.it/soluzioni-aziendali/siem-cos-e-come-garantisce-la-sicurezza-delle-informazioni/
[31] Intrusion Detection Systems: Snort, Palo Alto Networks, SolarWinds

con lo scopo di automatizzare la correlazione degli eventi derivanti da varie fonti e dare maggiore visibilità di cosa avviene e di chi ha causato l'azione. Questo servizio ha reso più efficiente la creazione delle segnalazioni anche grazie ai database aggiornati di IOC[32] che permettono la rivelazione automatica di potenziali minacce all'interno della rete. La grossa differenza sta nel fatto che le segnalazioni prima venivano generate solamente dopo aver attivato delle regole custom create dal SOC. Queste regole custom, possono essere di diverso tipo ed ancora oggi sono largamente utilizzate in quanto permettono di essere più specifiche e modulabili, in base a personalizzate correlazioni di eventi, a seconda delle esigenze.

Il SIEM da me utilizzato è stato IBM Security QRadar SIEM, "una piattaforma completa di security intelligence progettata per aiutare le aziende a gestire tutte le complessità dei loro processi operativi di sicurezza da una singola piattaforma unificata"[33].

Nel QRadar col quale ho lavorato, degli esempi di offense[34] (Fig. 4) che vengono generate dopo la rilevazione di una serie di eventi specificati in una custom rule, sono:

- Login Outside Operating Countries: nel momento in cui un'utenza effettua un'attività di login da un indirizzo IP dalla quale la sua azienda non opera.
- External Port Scanning: nel momento in cui un indirizzo IP esterno all'azienda, effettua una scansione.
- Kerberos Brute-Force: nel momento in cui un'utenza tenta l'accesso a determinati servizi, tramite protocollo Kerberos[35], inserendo ripetutamente una password riconosciuta come errata dal domain controller.

[32] Indicator of Compromise: artefatti riconosciuti malevoli, come "firme antivirali, un Indirizzo IP, un hash MD5 con cui si identifica univocamente un file malevolo, una URL e/o un nome di dominio da cui è stato veicolato un attacco o verso cui un malware si connette una volta attivato" (https://it.wikipedia.org/wiki/Indicatore_di_compromissione)
[33] https://www.ibm.com/it-it/topics/siem
[34] Nome specifico per gli alert generati da Qradar
[35] "In informatica e telecomunicazioni Kerberos è un protocollo di rete per l'autenticazione forte che permette a diversi terminali di comunicare su una rete informatica insicura provando la propria identità mediante l'utilizzo di tecniche di crittografia simmetrica." (https://it.wikipedia.org/wiki/Protocollo_Kerberos)

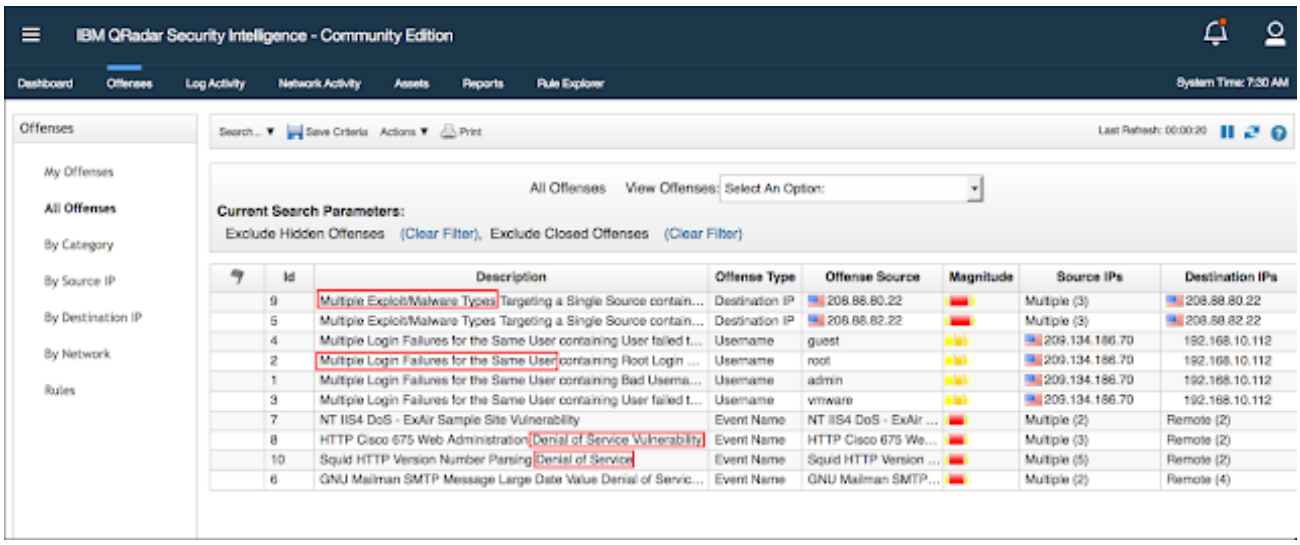

Figura 4 - Sezione "Offense" di IBM QRadar. FONTE: http://qradar4all.blogspot.com/2018/10/generate-log-events-for-qradar-ce-731.html

2.2. EDR

L'endpoint Detection and Response (EDR) è una tecnologia di cybersecurity che monitora i singoli dispositivi, al fine di rilevare e rispondere qualora vi sia la presenza di minacce.

Il termine è stato coniato nel 2013 da Anton Chuvakin, un cybersecurity specialist dell'istituto di ricerche tecnologiche Gartner di Stamford, Connecticut, con il quale voleva indicare tutti quei tool il cui focus erano i problemi legati agli host/endpoint[36].

A differenza di un SIEM, il focus dell'EDR non è il monitoraggio del traffico di una rete aziendale ma offrire servizi di prevenzione in base ad avanzati sistemi di threat detection. Questi sistemi partono dalle logiche di un classico antivurs e ne vanno a colmare i loro limiti. Nello specifico, la differenza sostanziale tra un antivirus ed un EDR sta nel fatto che il primo contiene un database di firme di attività malevole[37] costantemente aggiornato; il secondo, oltre a ciò, grazie a sistemi di machine learning, impara a riconoscerle ed applicare sistemi di prevenzione anche a contesti simili, non più solo per i casi contenuti nel database.

Da ciò si deduce che i limiti degli antivirus sono:

- Tempi di aggiornamento delle firme del database;
- Tempi di attesa prima dell'aggiornamento firme dell'agente locale;
- Attività malevole non contenute nei database non vengono rilevate, seppur magari simili ad altre presenti;

[36] https://en.wikipedia.org/wiki/Endpoint_detection_and_response
[37] Le firme includono delle caratteristiche specifiche di attività o file malevoli, veicoli di attacchi informatici, quali codici hash di file, stringhe di codice specifiche, estensioni file ed altro.

- Grossa esposizione ad attacchi “0-day”;
- Mancanza di storage dei log con conseguente possibilità di analisi retroattiva nel caso di minaccia rilevata;
- Mancanza di possibilità di ricerca attiva di potenziali minacce (non ancora inserite nei database) nella rete aziendale.

L’EDR riesce a colmare tutti questi difetti, andando ad aggiungere, inoltre, ulteriori strumenti, sia di rilevazione che prevenzione, utili ai reparti di sicurezza aziendali. Nello specifico, la presenza di un meccanismo di apprendimento e logiche di analisi più complesse, permettono di aver visibilità in tempo reale di situazioni di pericolo per un host. Partendo da un semplice file fino ad arrivare a command line sospette, seppur utilizzate da software leciti, viene tutto rilevato dall’EDR, in quanto il monitoraggio non è più basato sulle semplici firme.

Questi strumenti permettono la conservazione dei log e creano una correlazione degli stessi. Ciò è utile agli analisti in quanto permette di poter risalire in tempi rapidi alla radice di un problema rilevato, nonché di effettuare, qualora fosse necessario, ulteriori investigazioni ed approfondimenti.

Le analisi di questo tipo possono concretizzarsi anche in ricerche preventive. Tramite l’utilizzo di IOC, infatti, è possibile identificare quali macchine siano andate a contatto con file potenzialmente pericolosi o quali abbiano fatto ricerche verso domini e IP sospetti.

La tecnologia degli EDR è in continuo sviluppo e ciò ha permesso nel tempo l’aggiunta di utili funzionalità che permettono di avere un sempre maggior controllo dei dispositivi aziendali. Prima su tutti è la possibilità di instaurare una connessione da remoto agli endpoint. Grazie a questa connessione sarà possibile lanciare comandi da remoto, estrarre file, eseguire script custom ed effettuare analisi in dispositivi che potrebbero non essere raggiungibili fisicamente, in particolare al giorno d’oggi con l’incremento dello smart working.

Un’altra funzionalità è quella delle gestioni delle usb. Tramite la creazione di policy personalizzabili, si può gestire il mondo dei dispositivi removibili, andando a filtrare quali sono acconsentiti o meno ed anche decidendo quali modalità abilitare (lettura, scrittura o entrambe).

Concentrandosi nel campo degli incidenti, la capacità di isolamento di un endpoint rende gli EDR degli ottimi alleati in termine di prevenzione. Qualora fosse rilevata la compromissione di un uno di essi, ad esempio attraverso un malware, l’isolamento confina il problema al solo endpoint coinvolto, impedendone la diffusione all’interno della rete aziendale.

Procedendo poi con la creazione di policy di confinamento, si potrà decidere quale traffico abilitare, al fine di effettuare ulteriori analisi e ripulire la macchina infetta.

Durante il tirocinio, ho avuto modo di utilizzare diversi tipi di EDR quali Microsoft Defender for Endpoint, Symantec EDR e, con maggiore dettaglio, Falcon Crowdstrike (Fig.5). Questo strumento verrà approfondito nei prossimi capitoli ed utilizzato per effettuare delle analisi di trojan.

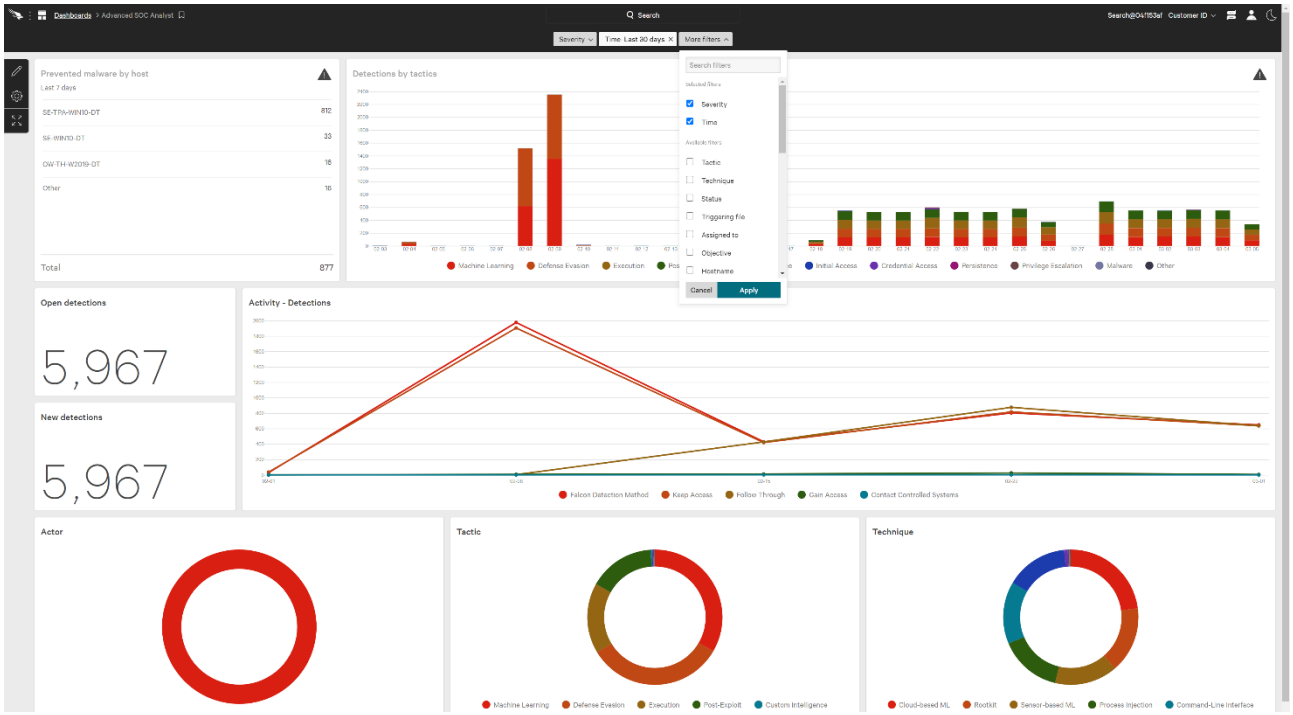

Figura 5 - Dashboard Falcon Crowdstrik. FONTE: https://www.crowdstrike.com/blog/tech-center/customizable-dashboards/

2.3. XDR

Come specificato nella sezione precedente, gli EDR limitano il loro controllo agli endpoint, non curandosi dell'interazione che avviene tra questi ed altri dispositivi all'interno della rete aziendale.

Lo sviluppo di una tecnologia che permettesse di coniugare la loro efficacia ed al contempo avere visibilità del traffico aziendale, è stato negli ultimi anni un obbiettivo primario per gli sviluppatori di questo tipo di strumenti.

Sono nati così gli XDR, ossia "eXtended Detection and Response", andando a contrassegnare un'evoluzione ed estensione degli EDR.

Non vi è una data di creazione vera e propria in quanto in un primo periodo, ma anche tutt'ora, il termine viene utilizzato con diverse accezioni, complice il fatto che la maggior parte dei diversi EDR cerca un modo per integrare a proprio modo la parte network mancante, con lo scopo di potersi dichiarare XDR ed avere quindi una maggiore visibilità e importanza nel mercato.

Per alcuni aspetti potrebbe essere visto come una fusione tra un SIEM e un EDR, per altri come l'integrazione di dispositivi di terze parti all'interno della stessa piattaforma, ed è proprio da queste funzionalità che sta prendendo sempre più forma la concezione di un XDR.

Le prime integrazioni utili a cui si può pensare sono quelle inerenti all'identity protection, ossia la protezione e monitoraggio dell'active directory[38]. Tramite questi moduli, gli amministratori di sistema possono controllare lo stato di salute ed effettuare personalizzazioni alle utenze senza doversi collegare da remoto ad un domain controller. È possibile, infatti, visualizzare i tempi di rotazione delle password o la loro compromissione, se sono stati effettuati accessi sospetti a servizi o file specifici, se vi sono utenze scadute ma non rimosse ma anche, in base allo strumento utilizzato, avere visibilità dei rischi del sistema: ad esempio, se possibile raggiungere privilegi elevati (non spettanti ad un'utenza base) tramite una serie di passaggi tra server e servizi che presentano delle vulnerabilità. Allo stesso modo, si possono anche applicare misure di sicurezza quali la revoca di sessione di un'utenza o il suo blocco, forzarne il rinnovo di una password o dell'MFA o obbligare l'utilizzo di quest'ultima per accedere a determinati servizi.

Il vantaggio di utilizzare un XDR, infatti, è la possibilità di effettuare operazioni e ricevere allarmi da differenti sorgenti di terze parti, tutto dalla stessa piattaforma. Come nel caso dell'identity protection, anche alcune impostazioni e regole di un firewall possono essere gestite tramite questo strumento. Si potranno così ricevere segnalazioni qualora un traffico sospetto sia rilevato dal firewall, andare a gestire le liste di gestione degli indirizzi IP o personalizzarne le policy.

Un altro esempio di integrazione è per l'email protection. Esistono tecnologie, come proofpoint[39], che permettono il monitoraggio del traffico mail e bloccare tutte quelle inerenti a spam o phishing, tramite meccanismi di intelligenza artificiale. L'utilizzo di un XDR permette la gestione anche di queste ultime ed, ancora una volta, la ricezione di segnalazioni tutte sulle stessa piattaforma, velocizzando così il lavoro degli analisti ed amministratori dei servizi.

Durante il mio tirocinio ho potuto utilizzare ed approfondire l'utilizzo di 3 XDR: Cynet, SentinelOne, Exabeam. Durante la loro gestione si nota sin da subito la diversa quantità di dati che questi strumenti devono gestire, a differenza di un EDR. Il vantaggio di poter disporre di eventi che non derivano solamente dall'host ma anche da altri tipi di sorgente permette di affrontare attività di threat hunting in modo più approfondito. Allo stesso tempo però, se chi li usa non è esperto nel settore IT/Network, si potrebbero riscontrare difficoltà ad analizzare tutti i dati, perdendo di vista l'obbiettivo finale.

Nel corso del tempo, però, anche alcuni EDR come Crowdstrike, stanno inserendo al loro interno alcune delle funzionalità viste precedentemente, espandendo la loro utilità e servizi offerti ad un pubblico più ampio.

[38] Sistema di server centralizzato che definisce la modalità con cui gli amministratori di sistema assegnano agli utenti le risorse di rete, tramite Group Policy ed i concetti di: account utente, account computer, cartelle condivise, stampanti di rete ecc (https://it.wikipedia.org/wiki/Active_Directory)
[39] https://www.proofpoint.com/it

CAPITOLO 3: CROWDSTRIKE

Crowdstrike è una compagnia americana di Cyberecurity, con sede ad Austin, Texas. Venne fondata da George Kutz, Dmitri Alperovitch e Gregg Marston nel 2011 e due anni dopo lanciarono il loro primo prodotto: l'EDR Crowdstrike Falcon.

Nel corso dell'ultimo decennio la società ha avuto modo di mettersi in luce nel campo della sicurezza informatica, in particolare a difesa degli Stati Uniti d'America. Ha collaborato sin dal 2014 col Dipartimento di Giustizia americano scovando diverse attività di cyber spionaggio effettuate da enti Asiatici, identificando hacker di ricercati gruppi di attivisti Russi e redigendo rapporti, nei quali venivano illustrati gli andamenti degli attacchi informatici nel panorama globale.[40]

Alcune delle immagini e analisi riportate nei paragrafi successivi sono state estratte durante il mio periodo di tirocinio, durante il quale ho potuto approfondire la mia conoscenza dello strumento tramite la gestione delle segnalazioni e le richieste ricevute da circa 30 clienti.

3.1. Introduzione all'EDR

Crowdstrike rilasciò la prima versione del loro EDR nel 2013, con l'obbiettivo di sostituire gli inefficienti antivirus, fornire supporto ad aziende che non possiedono un SOC, monitorare i dispositivi rimovibili, gestire log e rilevare vulnerabilità negli endpoint con l'agent installato; tutto ciò senza andare ad impattare sulle performance, grazie al funzionamento in cloud.

Per ogni funzionalità sopra citata, è possibile trovare un modulo specifico all'interno della piattaforma di Crowdstrike.

Falcon Prevent è il modulo di NGAV[41] che protegge dalle minacce digitali, compresi anche zero-day attacks e malware fileless, grazie a meccanismi di machine learning e intelligenza artificiale che

[40] https://en.wikipedia.org/wiki/CrowdStrike
[41] Next-Gen AntiVirus

analizzano i singoli processi e li correlano tra loro, rilevando i comportamenti sospetti o non attesi che si verificano e bloccandoli prontamente (Fig.6).

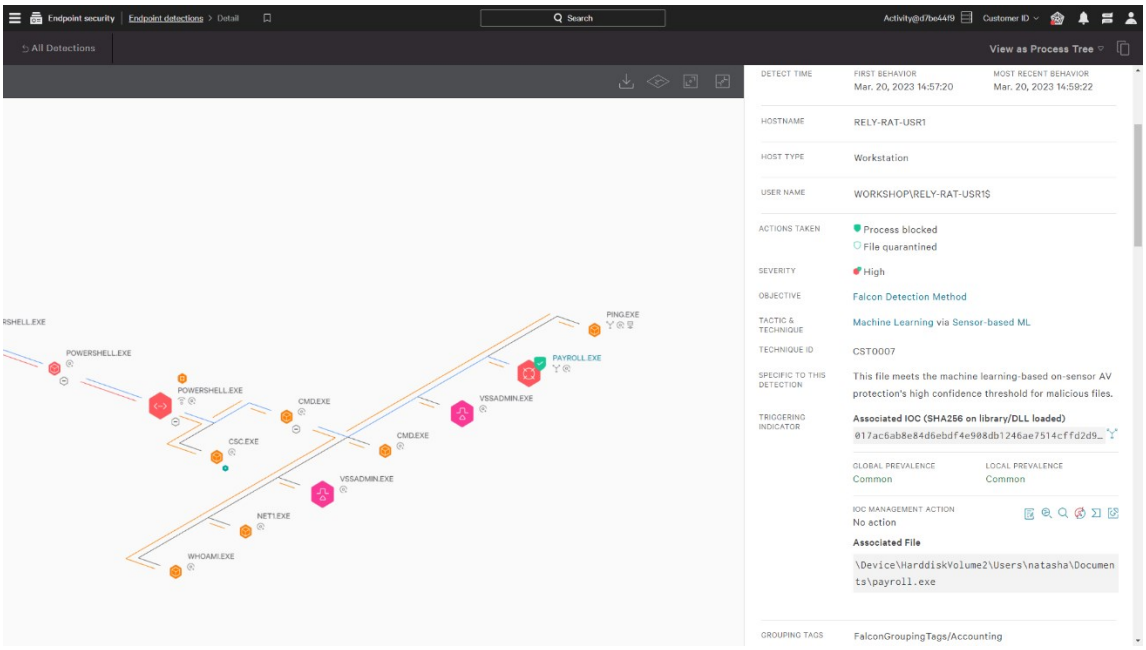

Figura 6 – Workflow di processi collegati e blocco preventivo di uno di essi. FONTE: https://www.crowdstrike.com/products/endpoint-security/falcon-insight-edr/

Con la sezione di Falcon Device Control è possibile monitorare l'utilizzo di tutti i dispositivi USB, veicolo tutt'oggi di potenziali minacce e soprattutto di attività di exfiltration[42]. Tramite Crowdstrike è possibile avere costante visibilità di tutti i dispositivi utilizzati ed applicare policy ad hoc in base alle esigenze. Quest'ultime includono opzioni di blocco preventivo per specifiche categorie di device, riconosciuti in piattaforma grazie al riconoscimento dei driver utilizzati (Audio/Video, Imaging, Mass storage, Mobile, Printer).

Falcon Spotlight evidenzia le vulnerabilità rilevate all'interno del proprio parco macchine. Ad ognuna di esse viene associata la relativa CVE[43] e possibile remediation applicabile, che sia essa un aggiornamento versione, patch o azioni correttive da effettuare tramite la gestione dei registri di sistema. Il tutto, utilizzando tecnologie di vulnerability assessment senza scansioni che, tramite un monitoraggio sempre attivo e a zero impatto sulle performance, permette di avere visibilità dei rischi in tempo reale.

Crowdstrike dispone di un team di esperti di threat intelligence che, tramite la telemetria ricevuta in cloud da tutti gli endpoint con l'agent installato, può effettuare analisi accurate e migliorare la prevenzione che l'EDR applica, anche riconoscendo attività malevoli ripetute da gruppi di cyber

[42] Attività con la quale vengono sottratti senza autorizzazione dati sensibili ad un'azienda e successivamente divulgati.
[43] Il Common Vulnerabilities and Exposures, o CVE è un elenco di vulnerabilità e falle di sicurezza note pubblicamente, per tutti i tipi di dispositivi e software. È gestito dalla MITRE Corporation. (https://it.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)

criminali (Fig.7) e dandone evidenza nella piattaforma agli analisti che dovranno gestire le segnalazioni.

Figura 7 - Segnalazioni crititche associate ai cybercriminali del gruppo "Berserk Bear". FONTE: https://www.crowdstrike.com/products/threat-intelligence/falcon-intelligence-automated-intelligence/

Crowdstrike ha migliorato negli anni la sua reputazione fino ad essere al giorno d'oggi uno degli EDR/XDR più efficaci e performanti, tanto da essere utilizzato da: 61 delle 100 aziende Fortune 100, 13 su 20 dei maggiori istituti bancari globali, dei 10 operatori sanitari e 7 delle 10 imprese energetiche più importanti.[44]

[44] https://www.crowdstrike.com/it/

3.2. Funzionamento in cloud

Un punto cardine del funzionamento di Crowdstrike è il suo sistema di cybersecurity interamente in cloud ed è stata una delle prime aziende a riuscire ad implementarlo.

I vantaggi sono molteplici, primo su tutti la leggerezza del sensore installato nelle macchine, di cui non ne impatta le performance in quanto il funzionamento è solamente quello di inoltrare la telemetria al cloud. I sensori, infatti, occupano meno di 20 Mb di memoria e sono disponibili per ogni tipo di endpoint: server, desktop/notebook o macchina virtuale.

Il sensore riconosce centinaia di tipi di eventi, li invia al cloud ed è lì che tutti i processi di calcolo vengono elaborati, dove vengono applicati meccanismi di IA e machine learning per scovare comportamenti tipici di malware, file o attività sospette ed andare a bloccare il tutto direttamente nell'host impattato.

Tutto ciò si traduce in oltre 5.000 miliardi di eventi a settimana[45], che possono essere visibili e gestiti (come anche le segnalazioni che ne derivano) da un'unica piattaforma sempre raggiungibile tramite internet. L'avere tutti i log online e centralizzati, inoltre, permettono di migliorare la ricerca e l'analisi di possibili nuove minacce degli analisti di Crowdstrike e delle sue logiche di interpretazione, andando così ad evitarle più velocemente, non avendo tempi persi per aggiornamenti di database di IOC.

Esistono anche applicazioni aggiuntive attivabili che, grazie alla telemetria che Crowdstrike fornisce, riescono ad esempio a creare uno storico di tutte le applicazioni, file e script di un endpoint, come Airlock Digital[46].

I requisiti per permettere la comunicazione tra agent e cloud sono il whitelist nei firewall aziendali del traffico TLS (1.0 o successivi) sulla porta 443 verso gli indirizzi di Crowdstrike, in base alla locazione aziendale, ossia:

- ts01-b.cloudsink.net (US-1)
- ts01-gyr-maverick.cloudsink.net (US-2)
- ts01-laggar-gcw.cloudsink.net (Organizzazioni del settore pubblico)
- ts01-lanner-lion.cloudsink.net (EU)

[45] https://www.tomshw.it/business/crowdstrike-la-sicurezza-it-interamente-in-cloud-per-sistemi-agili/
[46] https://www.airlockdigital.com/airlock-v4-5-released-linux-enforcement-agent-crowdstrike-integration-rbac-etc/

Al fine di garantire che questo tipo di traffico di rete da e verso il cloud rimanga sempre corretto ed inalterato, il sensore Falcon adotta il "certificate pinning"[47] come strumento di difesa da attacchi man-in-the-middle[48].

Per evitare interferenze con la verifica del certificato e problemi di performance, tuttavia, è necessario disabilitare la "deep packet inspection"[49] o altre impostazioni di rete simili che possono essere impostate nei firewall o server proxy.

[47] Tecnica di sicurezza che effettua una verifica di corrispondenza tra certificato/chiave pubblica e host che ci si aspetta di contattare.

[48] Comunemente nota come MitM, è una tipologia di attacco in cui qualcuno si inserisce nella comunicazione in corso tra due parti e ne altera il contenuto.

[49] Tecnica di ispezione dei pacchetti di rete volta alla ricerca di determinate firme all'interno dei payload e non solo nelle intestazioni. Può essere utilizzata per determinare problemi di performance di rete, verifica di firme malevoli, analizzare l'utilizzo delle varie applicazioni o la verifica che i dati siano in un formato corretto. (https://en.wikipedia.org/wiki/Deep_packet_inspection)

3.3. Installazione agent

Una caratteristica che ho potuto constatare nell'utilizzo di Falcon Crowdstrike è la costante ricerca di facilità d'uso e distribuzione dello strumento.

Per eseguire l'installazione dell'agent è sufficiente seguire una guida di pochi e semplici passi, a seconda della tipologia di sistema operativo con il quale si dovrà operare. I primi step comuni a tutti sono il download dell'installer del sensore dalla piattaforma online, basandosi sulla versione del SO e per i dispositivi Linux anche sulla alla versione del kernel, e il salvataggio del CID (Customer ID) ottenuto in fase di registrazione.

Per dispositivi Windows sarà sufficiente eseguire il file appena scaricato e seguire la procedura tramite GUI, specificando il CID (Fig.8).

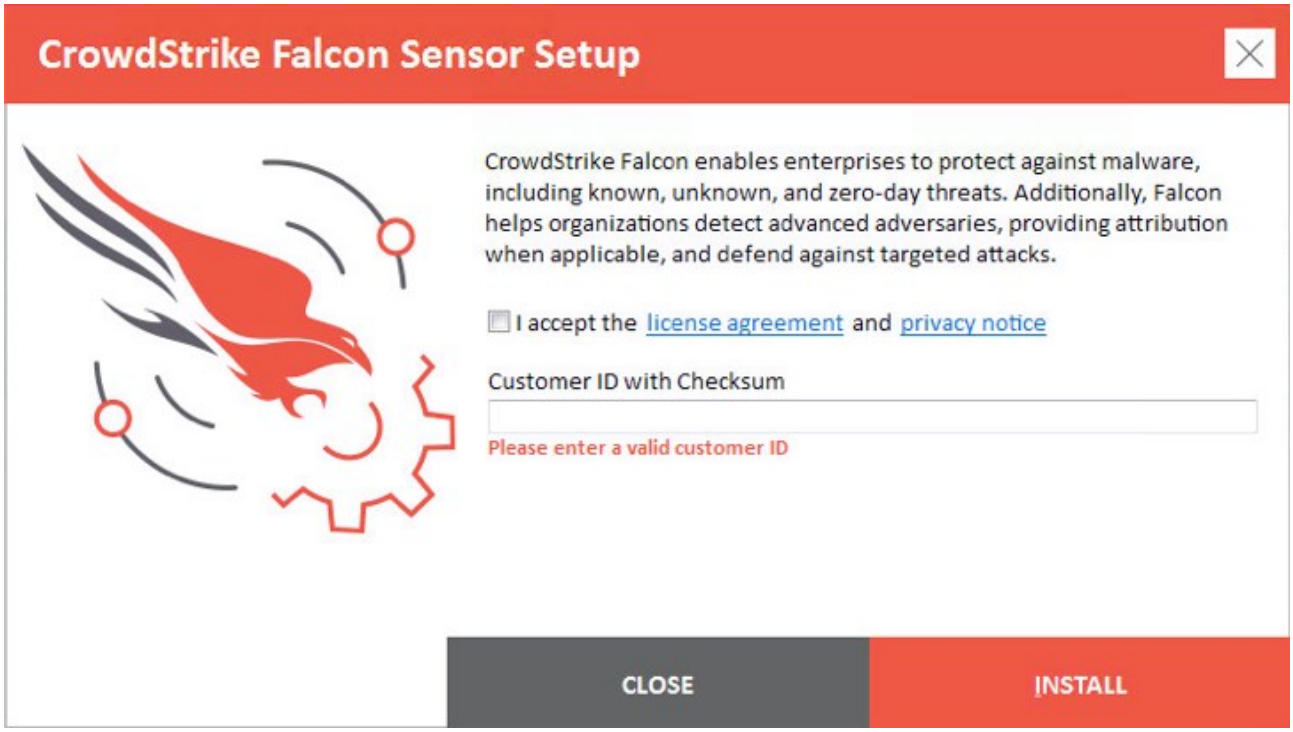

Figura 8 - Menù installazione agent Crowdstrike

Se l'installazione necessitasse di settaggi particolari, quali configurazione dell'indirizzo del proxy, l'aggiunta di un tag alla macchina o l'impostazione per le virtual machine, si potrà procedere mediante command line:

```
<installer_filename> /install /quiet /norestart CID=<CCID>
```

I parametri `/quiet` e `/norestart` indicano, rispettivamente, l'utilizzo dell'installazione senza UI e il non riavvio della macchina alla fine della stessa. Il riavvio, in generale, non è necessario e questo è un altro grande vantaggio del Falcon Sensor.

Per dispositivi Mac è suggerito il deploy tramite MDM[50] per automatizzare l'abilitazione dei permessi per il sensore, essendo un SO più restrittivo rispetto ai Windows.
Anche in questo caso però sarà sufficiente eseguire l'eseguibile del sensore o installarlo tramite command line:

```
sudo installer -verboseR -package <installer_filename> -target /
```

Per i device Linux, l'installazione va eseguita solamente tramite terminale, seguendo i seguenti passaggi:

1. Avviare l'installer, utilizzando il nome del file scaricato, con il corretto comando a seconda della versione in utilizzo:
   a. Ubuntu:
      ```
      sudo dpkg -i <installer_package>
      ```
   b. RHEL, CentOS, Amazon Linux:
      ```
      sudo yum install <installer_package>
      ```
   c. SLES:
      ```
      sudo zypper install <installer_package>
      ```
2. Impostare il CID nel sensore:
   a. Tutti i SO:
      ```
      sudo /opt/CrowdStrike/falconctl -s --cid=<CID>
      ```
3. Avviare il sensore:
   a. Host con SysVinit:
      ```
      service falcon-sensor start
      ```
   b. Host con Systemd:
      ```
      systemctl falcon-sensor start
      ```

Alla fine dell'installazione, il sensore contatterà il cloud e il nuovo host sarà automaticamente visibile dalla piattaforma, con il nome macchina associato al device.

Un ultimo aspetto di grande importanza, è che tutte le procedure possono essere effettuate anche se nei dispositivi sono già installati altre forme di protezione.
Dopo la fase di onboarding, che verrà approfondita nel capitolo successivo, Crowdstrike dovrà essere l'unico EDR presente nel dispositivo, fatta eccezione per Windows Defender che verrà disabilitato automaticamente, ma prima di ciò, l'installazione non avrà alcun impatto per la macchina.

[50] Mobile Device Management: attività di gestione dei dispositivi mobili aziendali, inclusi pc. Utile per gestire in modo univoco e distribuire policy o applicativi all'interno del parco macchine.

3.4. Le tre fasi di protezione

Dopo l'installazione dell'agent, l'EDR è operativo ed inizierà a monitorare le attività dell'endpoint, con un'aggressività in linea con la prevention policy in utilizzo.

Le prevention policy sono dei gruppi di regole di prevenzione personalizzabili che possono essere applicate a host specifici o gruppi di essi, in base alle esigenze. Questo tipo di policy contengono diversi parametri personalizzabili che vanno a modificare il comportamento e l'aggressività dell'EDR in fase di analisi delle attività. Sono inoltre suddivise nei 3 sistemi operativi (Microsoft, Mac, Linux), in quanto ognuno di essi avrà un diverso numero di opzioni da impostare.

Dalla schermata delle prevention policy (Fig.9) è possibile crearne di nuove ed editarne la precedenza, in modo tale che, se un host sia presente in più di esse allo stesso momento, recepisca le impostazioni solamente di quella con la precedenza maggiore.

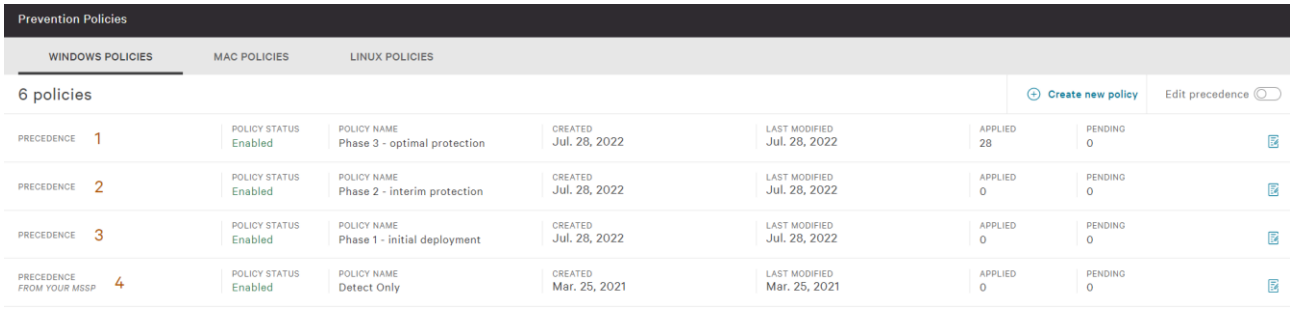

Figura 9 - Sezione Prevention Policy per macchine Windows.

Le opzioni attivabili sono innumerevoli e vanno dal controllo delle PowerShell utilizzate, monitoraggio del traffico HTTP/HTTPS in uscita dall'host, scansione della memoria per rilevare in-memory attacks[51], gestione sospetta delle immagini del BIOS, gestione della quarantena, monitoraggio attività pre-ransomware, tentativi di exploit e blocco di software che cercano di estrarre credenziali.

Durante il periodo di tirocinio ho potuto seguire l'onboarding per alcuni nuovi clienti, diviso inizialmente nella fase di deploy dell'agent per i vari dispositivi delle aziende e successivamente nell monitoraggio delle segnalazioni generate dagli stessi.

L'applicazione sin da subito delle logiche di prevenzione dello strumento, però, potrebbe impattare il normale flusso di lavoro aziendale, in quanto sussiste il pericolo che Crowdstrike vada a rilevare come sospetti alcuni processi invece leciti e necessari. Falcon Prevent, ad esempio, potrebbe riconoscere come malevoli alcuni file di Office365 con macro al loro interno (principale veicolo di attacchi derivanti da phishing), script interni custom necessari alla gestione di risorse nei server o,

[51] Cyber attacchi che possono installarsi tramite o senza file associati e "lavorano" nel lasso di tempo in cui specifiche applicazioni vengono utilizzate, per poi fermarsi quando vengono spente anche loro.

peggio ancora, altri utilizzati per gestire macchinari aziendali ed andare a bloccare una linea produttiva.

Per ovviare a tutto ciò, si procede tramite l'applicazione di una procedura a 3 fasi: utilizzando 3 differenti prevention policy (Fig.9), con severity di monitoraggio e prevenzione crescente, si potrà gestire l'onboarding evitando i problemi sopracitati, con il costante e necessario feedback dei clienti.

Le 3 policy sono diverse tra loro per il settaggio delle varie opzioni sopracitate ed in particolare per la sezione inerente alla severity applicata ai meccanismi di machine learning, sia dal cloud che dal sensore.

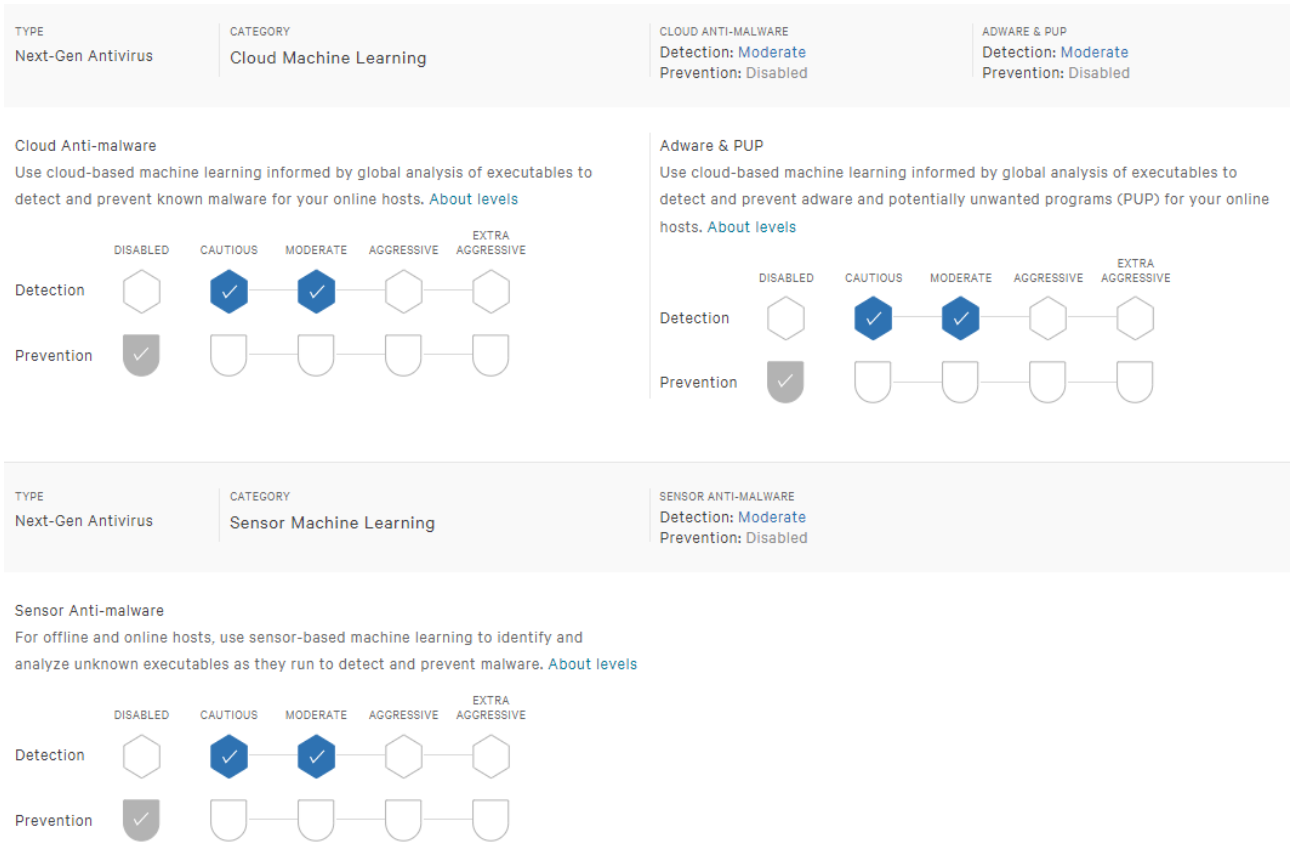

Figura 10 - NGAV Severity Policy (Phase 1)

Nella "Phase 1 – Initial Deployment" vengono inseriti i primi host di test, ai quali vengono applicati controlli (detection) moderati e nessun tipo di prevenzione (Fig. 10).

Trascorsi una decina di giorni ed applicati i primi whitelist necessari, in base alle segnalazioni rilevate dalla piattaforma, gli host possono essere spostati in "Phase 2 – Interim Protection", dove recepiranno l'inserimento di una prevenzione moderata e un innalzamento in "aggressive" della detection. Questa fase è cruciale in quanto è la fase finale di coesistenza con un altro antivirus/EDR, qualora dovesse esistere nell'host. Non impostando la prevenzione ad alti livelli, infatti, non si rischia di creare

interferenze fra i due sistemi di protezione e si può continuare l'attività di tuning[52] per altri circa 10 giorni, prima di passare alla terza fase, la policy "Phase 3 – Optimal Protection".

Raggiunta questa fase, la severity applicata per detection e prevention sarà settata in "aggressive" e Crowdstrike dovrà essere l'unico EDR installato, ultimando così, la fase di onboarding.

3.5. Detections & Prevention

Un cyber attacco è tipicamente costituito da una sequenza di azioni elencate nella "Cyber Kill Chain"[53], un modello utilizzato per identificare la struttura di un attacco e bloccare le attività nemiche, ispirandosi all'approccio militare. La Cyber Kill Chain, sviluppata da Lockheed Martin nel 2011, è composta da 7 fasi: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control e Action on Objective. Inizialmente, gli attori degli attacchi effettuano attività di ricerca di informazioni sul loro target, come la raccolta di indirizzi IP, porte esposte, indirizzi e-mail, dettagli del parco macchine ed altro, al fine di potersi attrezzare al meglio durante la seconda fase, nella quale crea i vettori di attacco, quali malware, ransomware, virus, worm. La fase di delivery consiste nell'inizio dell'attacco, tramite, ad esempio, la consegna di una mail di phishing studiata ad hoc con le informazioni ottenute precedentemente. Nel quarto step, il codice malevolo attivato viene eseguito e, se non bloccato, dà il via alla fase successiva di installazione ed il permesso all'attaccante di iniziare ad assumere il controllo del sistema. Quest'ultima azione si concretizza nella fase di "C&C", ossia il completo controllo del dispositivo o identità rubata, per proseguire con attività di "lateral movement"[54]. Si hanno evidenze dal raggiungimento della fase finale tramite i danni che l'azienda bersaglio subisce concretizzabili in furto di dati, distruzione di alcuni di essi o la loro criptazione e la successiva richiesta di riscatto, come per i ransomware.[55]

Ogni tipo di piattaforma utilizza una propria specifica nomenclatura per delineare ciò che in generale sono gli alert. Crowdstrike li definisce come detection e vengono generate al momento della rilevazione di un'attività sospetta, riconducibile ad una delle ultime 4 fasi della Cyber Kill Chain.

Tramite le detection è possibile tenere monitorato le attività insolite che avvengono negli host della rete sotto controllo. In figura 11 è possibile vedere la sezione inerente ad esse all'interno della piattaforma.

[52] Attività di modifica delle regole di whitelist al fine di impedire il blocco di particolari applicativi necessari.
[53] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[54] Attività durante la quale gli attaccanti spostano il controllo da remoto da una macchina all'altra, estendendo così l'infezione all'interno dell'infrastruttura bersaglio.
[55] https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/

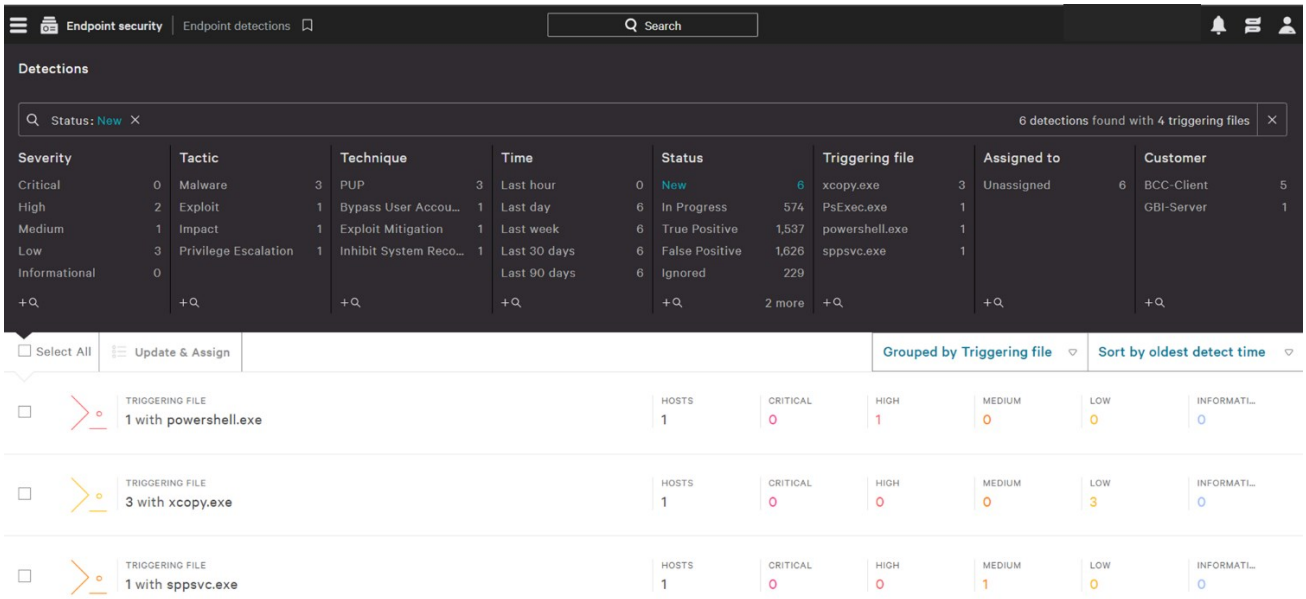

Figura 11 - Dashboard Detection Falcon Crowdstrike

Da qui è possibile apporre dei filtri alle segnalazioni, in base al nome della macchina, tempo di rilevamento, file sospetto rilevato ed altri; sia tramite alcuni preimpostati, che dalla barra di ricerca.

Andando ad espandere una detection, verrà mostrata una finestra con tutti i dettagli necessari a condurre un'analisi. In figura 12 ve ne è una prima parte, in cui viene indicata l'attività di prevenzione applicata e la categorizzazione della minaccia, in accordo con le tecniche e tattiche del framework "Mitre Att&ck". Queste categorie sono raggruppate in 6 "Objective": Gain Access, Keep Access, Explore, Contact Controlled Systems, Follow Through, Falcon Detection. Ognuno di questi oggetti viene usato come riferimento alle diverse fasi della Cyber Kill Chain, tranne per l'ultimo che raccoglie eventi specifici riconosciuti dall'IA di Crowdstrike e considerati di particolare rilievo quali Malware.

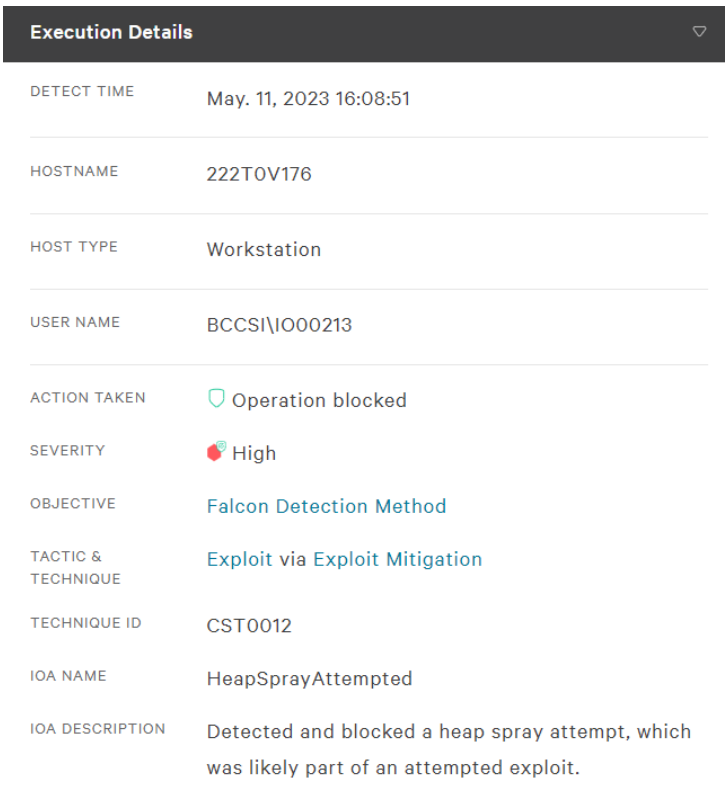

Figura 12 - Descrizione e categorizzazione detection

Scorrendo nella finestra della detection, sarà possibile vedere tutte le attività inerenti ad essa, come: operazioni effettuate sul disco, modifiche ai registri, path dei file, commandline utilizzata, chiamate DNS, processi di sistema.

Vi è inoltre un pulsante per l'isolamento tempestivo dell'host, qualora una sua reale compromissione venisse rilevata ed un altro che permette di accedere alla visualizzazione ad albero della sequenza di attività fatte prima di arrivare alla detection stessa (Fig.13).

Figura 13 - Threat Graph della minaccia rilevata da Crowdstrike.

Per ogni passo è possibile vedere lo stesso menù illustrato in figura 11 ed avere così evidenza, uno step alla volta, di tutto il processo dettagliato. L'ultimo di essi illustra l'attività sospetta effettuata da una powershell. Dalla segnalazione si evince che powershell è stata utilizzata tramite la command line:

```
powershell.exe -file "C:\Program Files (x86)\starterwebprd\.\cfg\tscmd.ps1
```

Ciò ha comportato all'utilizzo di driver dll e alla scrittura di un ulteriore file: "`PSScriptPolicyTest_p5y43pf5.u32.ps1`".

Seppur si possa presumere che esso non sia malevolo, basandosi sul fatto che il nome riconduce ad attività di test, la creazione di un secondo file con estensione ps1[56] e l'allocazione di memoria ad esso conseguita, possono ricondurre ad un tentativo di heap spray. Questa tecnica è utilizzata per eseguire arbitrariamente codice in un sistema infetto, dopo aver causato errori all'interno dello stesso tramit e l'overflow dell'heap memory[57].

Come evidenziato nel campo "Action Taken", l'EDR è intervenuto bloccando questa attività; ciò rientra nella categoria delle prevenzioni. Le altre possibili azioni previste sono la quarantena di file sospetti e, se essi dovessero aver generato ulteriori file o modifiche ai registri durante la loro installazione, anche una fase finale di remediation, nella quale il sistema viene ripristinato allo stato precedente dell'installazione, tramite la rimozione di tutte le modifiche rilevate causate dal file. In figura 14 si riporta un esempio di quest'ultima casistica ove il file "BrytonUpdateTool (2).exe" è stato riconosciuto come sospetto, bloccato, quarantenato e causato l'attivazione della remediation da parte dell'EDR.

[56] Estensione utilizzata per script di powershell.
[57] Blocco di memoria dinamico assegnato ai programmi per permetterne l'esecuzione.

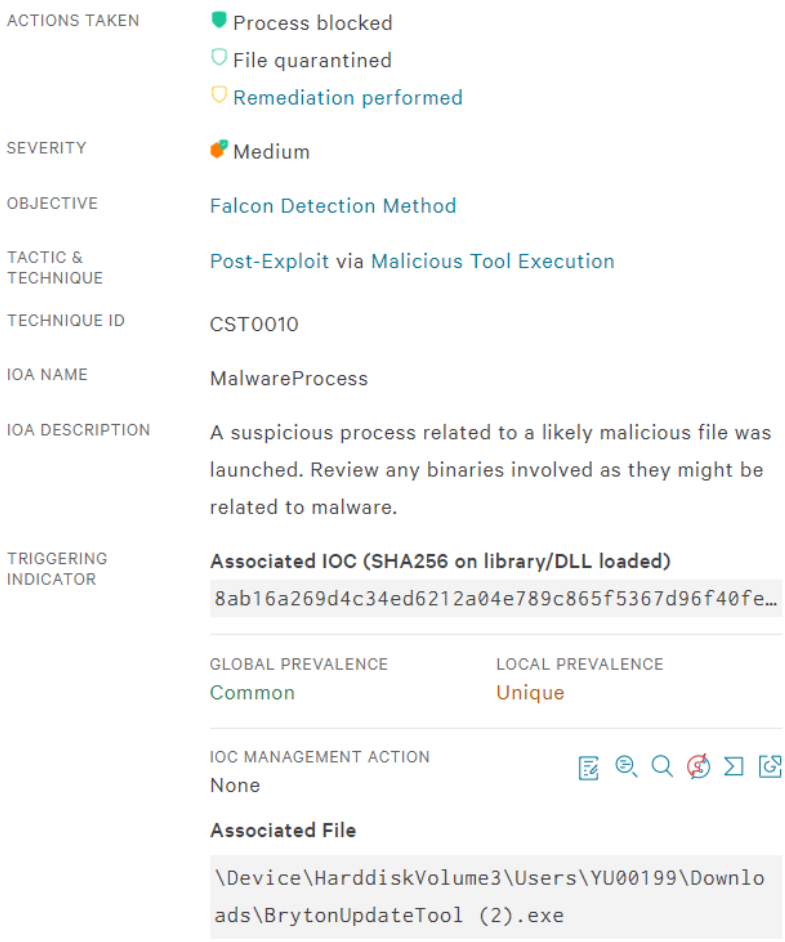

Figura 14 - Detection e prevention di un file eseguibile sospetto

CAPITOLO 4: SANDBOX TROJAN

In questo capitolo verranno illustrate le tecniche utilizzate dai SOC ed esperti di cybersecurity per effettuare analisi comportamentali dei malware, con particolare riferimento ai Trojan ed ai loro meccanismi di infezione delle macchine.

Le stesse attività sono state da me riprodotte durante il percorso di tirocinio, utilizzando macchine virtuali isolate e moduli di Crowstrike atti a questo tipo di analisi, per svolgere un'analisi sul Trojan Andromeda. Durante le analisi sono stato indirizzato da colleghi con più esperienza nel settore che hanno verificato la correttezza delle informazioni riportate e mi hanno permesso di approfondire le mie conoscenze in materia.

4.1. Introduzione Sandbox

Un primo metodo di approccio all'analisi di un malware, o in generale di un software sospetto, è quello di eseguirlo all'interno di una sandbox.

Le sandbox sono macchine virtuali nelle quali è possibile eseguire applicazioni o processi in modo sicuro, senza che possano avere impatti nella rete aziendale. Vengono utilizzate per testare software, eseguire codice non attendibile o isolare applicazioni potenzialmente dannose.

Una loro peculiarità è quella di poter essere collegate ad internet ed al contempo isolate dal resto dell'infrastruttura aziendale, con accesso limitato alle risorse di rete. Questo meccanismo può essere applicato utilizzando tecniche come la segmentazione di rete, la creazione di regole firewall o l'utilizzo di VPN per stabilire connessioni sicure con l'esterno. La connessione ad Internet, invece, può essere implementata tramite una connessione di rete separata da quella dell'azienda, tramite una linea dedicata o una rete virtualizzata.

Al giorno d'oggi, esistono anche strumenti online per effettuare questi tipi di test. Sono sandbox create per eseguire in automatico i file che vengono caricati e creare un report dell'attività rilevata da essi derivante, evidenziando comportamenti dannosi di malware, connessioni sospette, tentativi successivi di exploit ed altre azioni malevole.

Crowdstrike fornisce il servizio "Falcon Sandbox"[58] per effettuare analisi profonde di minacce, arricchendo i risultati forniti tramite meccanismi di Cyber Threat Intelligence e fornendo IOC utilizzabili per migliorare le difese del proprio asset. Grazie a questo tipo di informazioni inserite nei report dei risultati, gli analisti che utilizzano il tool di Crowdstrike, potranno capire in modo più rapido il contesto di utilizzo di determinate minacce. Ad esempio, possono essere integrate

[58] https://www.crowdstrike.com/products/threat-intelligence/falcon-sandbox-malware-analysis/

informazioni inerenti ai gruppi di hacker che sfruttano determinati software o exploit e come rilevare in modo preventivo le loro attività, o infezioni da essi derivanti.

4.2. Malware Trojan

Tra le minacce più diffuse e pericolose si trovano i Trojan, o "cavalli di Troia", che rappresentano una forma sofisticata di malware progettato per infiltrarsi in un sistema informatico, presentandosi come un'applicazione o un file apparentemente legittimo, al fine di danneggiare, rubare dati o assumere il controllo del sistema stesso.

Esistono diverse categorie di Trojan, ciascuna focalizzata su un obiettivo o una funzionalità dannosa specifica. Ad esempio, i Trojan bancari sono progettati per rubare le credenziali di accesso bancarie e altre informazioni finanziarie sensibili. I Trojan di accesso remoto (RAT) consentono agli attaccanti di assumere il controllo remoto dei sistemi infetti, consentendo loro di monitorare le attività dell'utente e acquisire informazioni sensibili. I Trojan backdoor aprono una backdoor nei sistemi infetti, fornendo agli attaccanti un accesso non autorizzato in qualsiasi momento. I Trojan downloader scaricano e installano altri malware sui dispositivi infetti.

I Trojan possono essere diffusi in diversi modi, tra i quali il download di software pirata, o da fonti non ufficiali, o il download di materiale da fonti non attendibili, ma il meccanismo di diffusione più utilizzato, come per la maggior parte dei malware, è il phishing. Tramite l'invio di mail contraffate, contenenti link che reindirizzano a siti malevoli o documenti con macro nascoste, gli attaccanti sono in grado di utilizzare vulnerabilità presenti nel browser o nel sistema operativo dell'utente per eseguire codice dannoso senza il suo consenso. Questo può includere l'utilizzo di exploit noti o zero-day per sfruttare le vulnerabilità non ancora corrette.

Una volta sfruttate le vulnerabilità, il Trojan viene scaricato e installato nel sistema dell'utente senza la sua consapevolezza. Dopo l'installazione, il Trojan cercherà di garantire la sua persistenza nel sistema, ad esempio, modificando i registri o le impostazioni del sistema. Successivamente, al raggiungimento di determinate condizioni si attiverà e inizierà a svolgere le sue funzionalità dannose.

4.3. Andromeda

Il Trojan Andromeda, noto anche come Gamarue, è stato uno dei Trojan più diffusi e dannosi che ha colpito i computer in tutto il mondo. Ha avuto un'ampia diffusione nel periodo compreso tra il 2011 e il 2017, anno nel quale la sua attività è stata interrotta grazie a un'operazione congiunta delle forze dell'ordine e delle società di sicurezza informatica.

Una volta che il Trojan Andromeda si insediava all'interno di un sistema, utilizzava una serie di meccanismi sofisticati per evitare la rilevazione e la rimozione da parte delle soluzioni di sicurezza. Tra le tattiche utilizzate c'erano la criptazione del codice malevolo, l'utilizzo di rootkit per nascondere la sua presenza e l'injection di codice dannoso all'interno dei processi legittimi del sistema operativo.

Andromeda si insediava nei PC sfruttando le vulnerabilità dei software o sfruttando le credenziali di accesso deboli. Una volta compromesso un sistema, il Trojan stabiliva una comunicazione con il server di comando e controllo (C&C) dell'attaccante per ricevere istruzioni e inviare i dati raccolti dal sistema infetto. Questo permetteva agli attaccanti di assumere il controllo remoto del sistema, raccogliere informazioni sensibili, installare altri malware o sfruttare il computer per condurre attacchi DDoS (Distributed Denial of Service). Tra le varie attività che potevano essere eseguite, lo scopo principale era quello finanziario. Gruppi di criminali informatici utilizzavano il Trojan per sfruttare i dati personali degli utenti, come informazioni bancarie o credenziali di accesso, al fine di compiere frodi finanziarie o estorcere denaro.

La diffusione su larga scala di Andromeda ha causato danni significativi a livello mondiale, compromettendo la sicurezza dei sistemi informatici, mettendo a rischio la privacy degli utenti e creando una delle più longeve botnet, utilizzata per la diffusione di virus informatici. Questo fino al 2016, anno in cui la Procura della Repubblica di Verden, la Polizia di Luneburg, FBI, Europol ed Eurojust rilevarono l'infrastruttura Avalanche, utilizzata per lanciare malware globali, tra i quali Andromeda. Dopo questa prima scoperta, le autorità giudiziarie di 15 Paesi iniziarono un takedown coordinato dei sistemi infetti, che porto alla fine dell'espansione ed utilizzo del malware[59].

4.4. Analisi Andromeda tramite Falcon Sandbox

L'obiettivo del capitolo è quello di analizzare il Trojan Andromeda mediante l'utilizzo della sandbox di Crowdstrike illustrata nel capitolo 4.1. Questa attività è stata svolta durante il mio tirocinio ad HWG, durante il quale ho avuto accesso alla Falcon Sandbox ed ho potuto elaborare le seguenti informazioni.

Dopo aver caricato nella sandbox l'eseguibile, viene effettuata l'analisi del malware fornendo dettagli sull'attività che esso svolgerebbe all'interno di una macchina infetta.

Dal report viene riconosciuto il file come malevolo con uno score di 100/100 e vengono riconosciuti dei collegamenti con i Trojan, Andromeda and Gamarue (Fig.15).

[59] https://www.repubblica.it/cronaca/2017/12/08/news/cybercrimine_blitz_polizia-fbi_contro_hacker_della_rete_andromeda_-183462911/

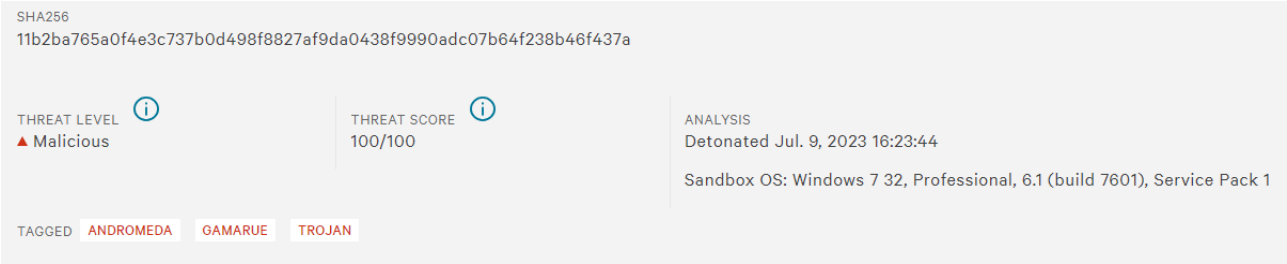

Figura 15 - Valutazione Malware tramite Falcon Sandbox

La prima sezione del report riguarda i "Risk Assessment", attività malevoli che creano rischi all'interno dei sistemi. Ad Andromeda sono stati associati meccanismi di persistenza, fingerprint, evasione, comportamenti di rete.

La persistenza include quelle attività per le quali il malware cerca di instaurarsi nella macchina infetta, di non essere rilevato e di potersi eseguire autonomamente. Per fare ciò, vengono scritti byte malevoli all'interno del processo lecito di sistema "C:\Windows\System32\wuauclt.exe", utilizzato per la verifica della disponibilità di aggiornamenti Windows[60] (Fig.16).

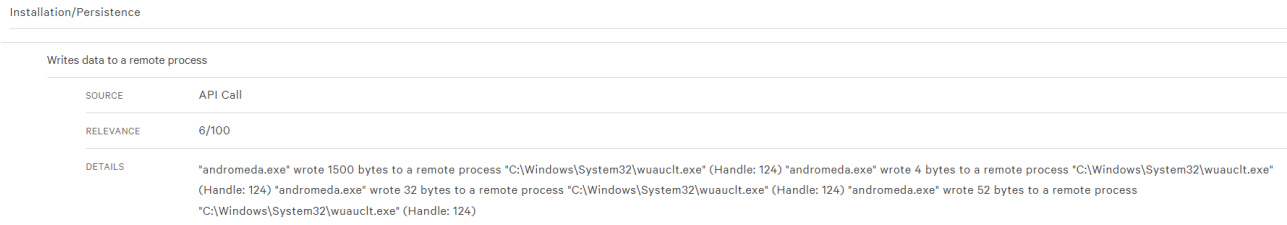

Figura 16 - Injection eseguita in wuauclt.exe

Normalmente, questo tipo di attività verrebbe rilevata dagli antivirus, in quanto corrisponde ad attività di injection. Per bypassare il controllo però, la modifica al codice dell'eseguibile viene fatta dopo aver creato il processo in modalità di sospensione. In questo modo è possibile bypassare i controlli, in quanto i processi sospesi non vengono monitorati attivamente ed una loro attivazione in un secondo momento fa sì che vengano accettati e riconosciuti come leciti, seppur con modifiche al loro interno. Dopo essere stato silenziosamente modificato, vengono rilevate delle chiamate API[61] a

[60] https://www.tosolini.info/2011/07/windows-update-server-wuauclt-exe-parametri/
[61] "La chiamata API è un processo attraverso il quale due software scambiano dati. Quando un'applicazione fa una chiamata API, invia ad un'altra applicazione una richiesta specifica che viene ricevuta e processata da una API." (https://openapi.it/blog/cosa-e-chiamata-api.html)

"ZwResumeThread", per permettere la ripresa del thread/processo. A questo punto, "wuauclt.exe" a sua volta modifica la dll "wshtcpip.dll" (Fig.17), utilizzata per la gestione dei socket, andando a creare le basi per l'instaurazione di una sessione di C2C con un server remoto.

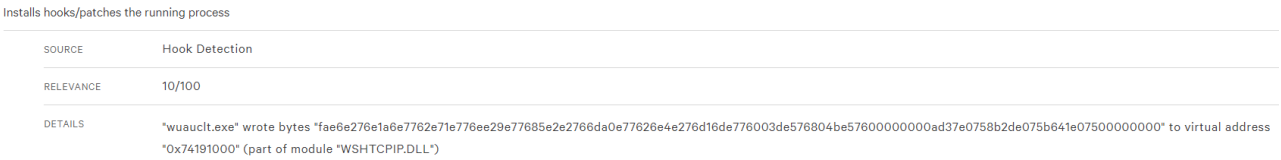

Figura 17 - Modifica di wshtcpip.dll

Inoltre, esso crea il processo "C:\ProgramData\Local Settings\Temp\msvewoqiy.exe" ed afferma la propria persistenza modificando i registri per permettere l'auto-esecuzione dello stesso (Fig.18). Un requisito necessario per definire un Trojan è che la sua esecuzione non venga rilevata dall'utente e così accade, in quanto si nascondono dietro processi leciti, come quello per l'aggiornamento del pc.

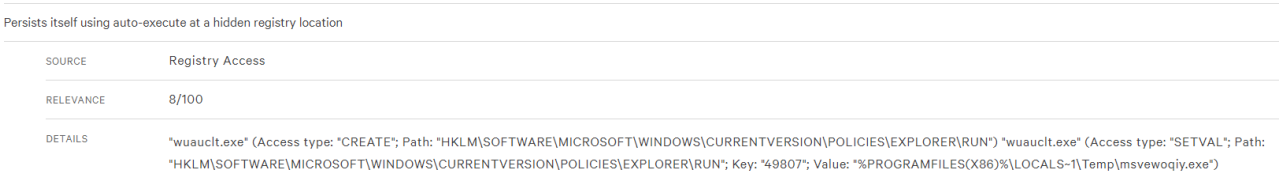

Figura 18 - Persistenza effettuata tramite auto-esecuzione

Dal report si può capire anche che alcuni file PE[62] contengono contenuti criptati, in quanto la loro entropia è 7.76 (valutata in una scala da 1 a 10)(Fig.19).

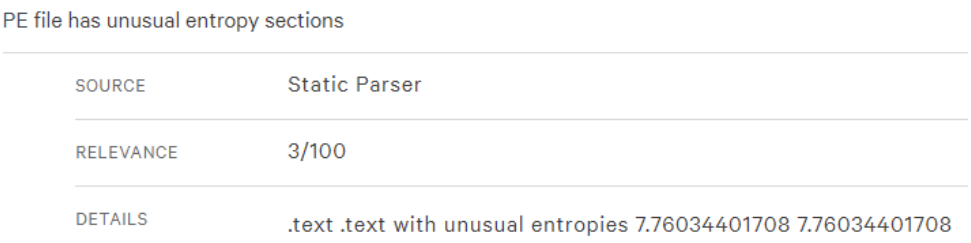

Figura 19 – Anomala alta entropia di file PE

Tramite le sessioni di C2C, l'attaccante cerca di ricavare le informazioni della macchina impattata, nello specifico l'indirizzo IP (Fig.20), tramite l'utilizzo di URL di diverso tipo scritti in memoria ed effettuando quindi connessioni di rete.

[62] Portable Executable (PE): formato di file per DLLs, eseguibili ed altri oggetti utilizzati dai sistemi operativi Windows.

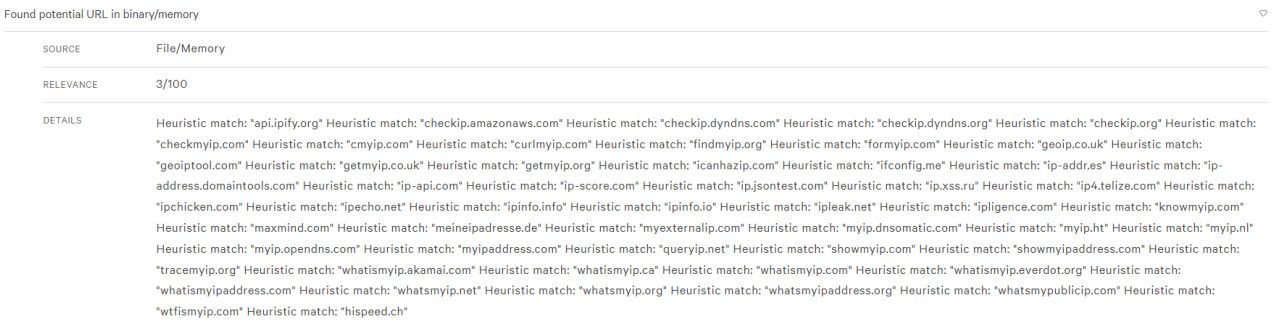

Figura 20 - Fingerprint indirizzo IP host infetto

Infine, le tecniche di evasione consistono in attività di verifica svolte dal malware, per determinare la tipologia di ambiente nel quale si sta eseguendo. Se dovesse rilevare una virtualbox, ad esempio, sono presenti meccanismi di autoeliminazione, al fine di non permettere il reverse-engineering del codice da parte degli analisti. La stessa tipologia di attività viene svolta da wuauclt.exe (dopo aver subito le modifiche illustrate precedentemente) per rimuovere l'eseguibile "andromeda.exe" ed eliminare ogni traccia dell'inizio dell'infezione (Fig.21).

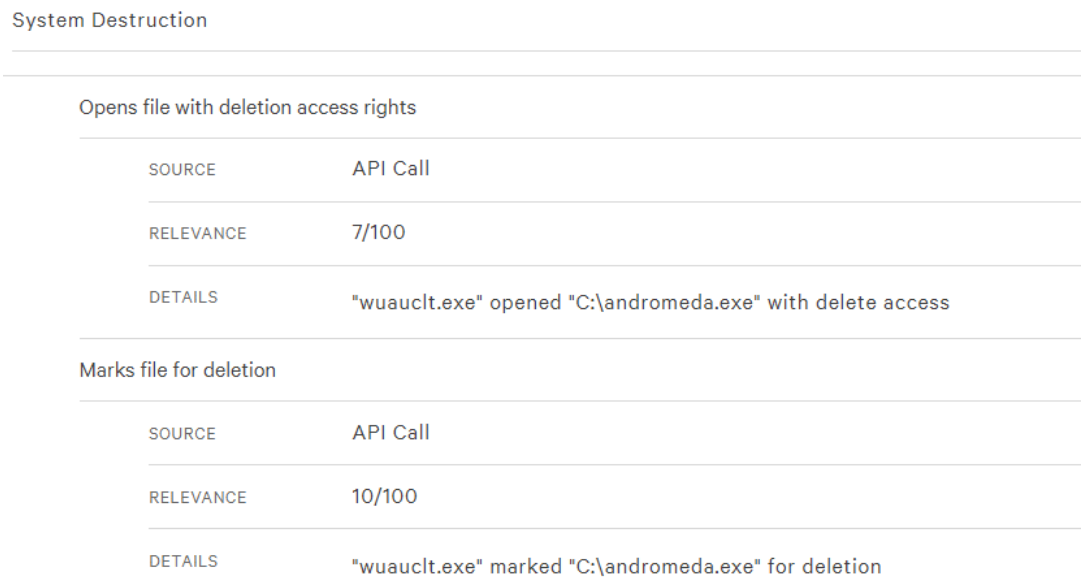

Figura 21 - Evasion effettuata tramite rimozione degli eseguibili sospetti

4.5.Rilevamento tramite EDR Crowdstrike ed isolamento endpoint

Crowstrike EDR, per limitare l'utilizzo di risorse, non effettua scansioni passive all'interno delle macchine per verificare il contenuto di ogni file ma effettua tale attività nel momento in cui i file vengono maneggiati, anche se per una sola copia senza apertura. Ad esempio, se all'interno di un pc vi fossero file malevoli e venisse installato l'agent di Crowdstrike, essi non verrebbero rilevati, fino al momento in cui non vengano utilizzati.

Nel momento in cui “andromeda.exe” viene lanciato, l’EDR interviene istantaneamente (Fig.22), rilevandolo staticamente tramite machine learning come malware ma anche dinamicamente a livello comportamentale, associandogli attività di “Execution” utilizzando “Command and Scripting Interpreter”, ossia l’esecuzione di codice/script tramite interpreti di linguaggi. L’attività viene dunque interrotta e il file messo in quarantena, senza ripercussioni nel sistema.

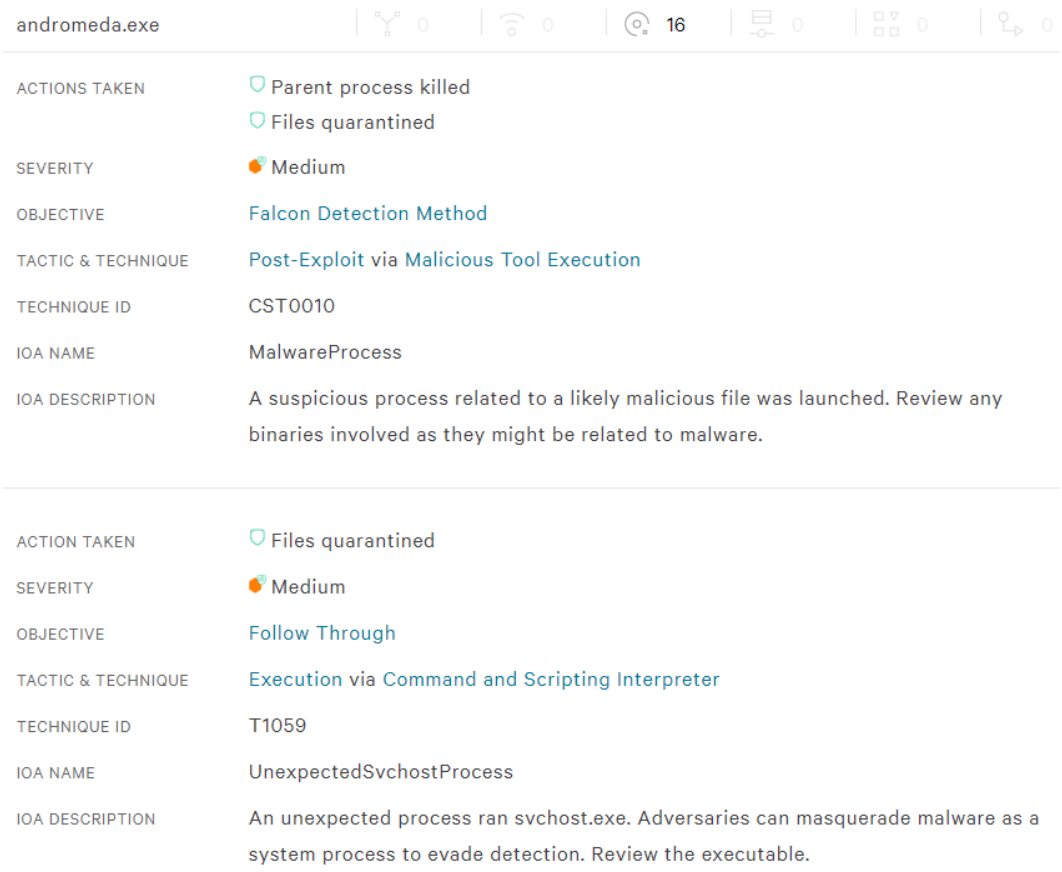

Figura 22 - Detection tramite Crowdstrike dovuta al rilevamento di Andromeda

L’analista del SOC che analizzerà il caso dovrà valutare l’entità della minaccia e se venisse rilevato lo stato di compromissione della macchina coinvolta, col conseguente rischio che l’infezione si propaghi all’interno della rete aziendale, dovrà procedere con l’isolamento della stessa.

Per fare ciò, l’EDR offre il pulsante “Network Contain” nella schermata della detection e, dopo aver confermato la richiesta (Fig.23), l’host verrà isolato dalla rete.

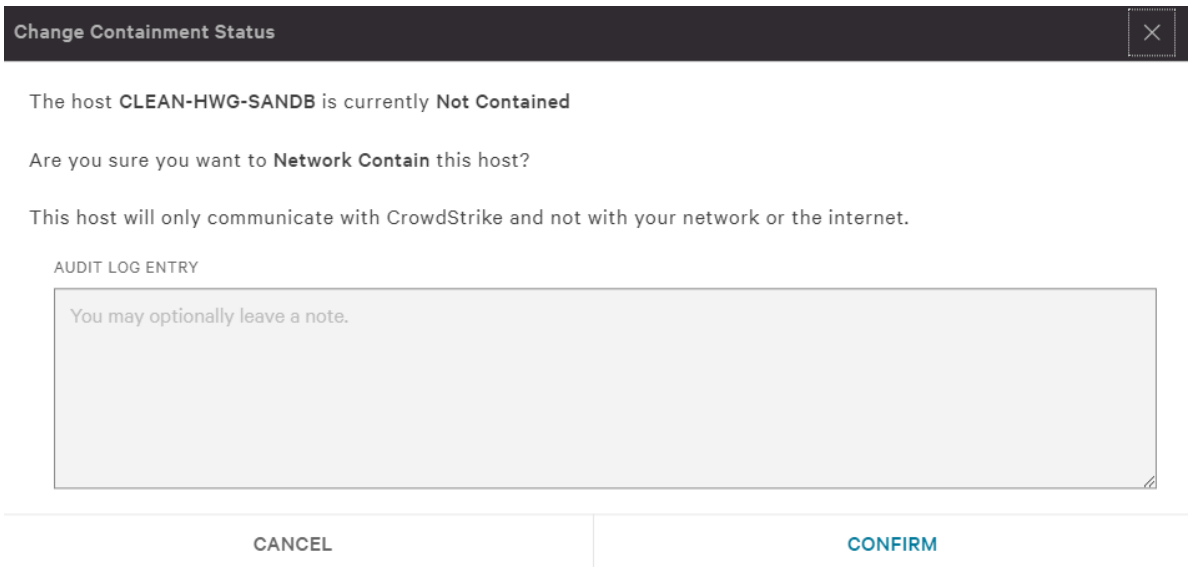

Figura 23 - Conferma network containment

Esso comunicherà con il cloud di Crowdstrike, per permettere di non perdere le informazioni utili al suo interno ed anche poter creare una sessione in RDP per poter operare all'interno dello stesso da remoto ed in sicurezza. In alternativa, potrà essere configurata una policy di contenimento, grazie alla quale si potranno specificare quali indirizzi IP l'host isolato potrà raggiungere ed anche quali potranno raggiungere lo stesso.

CONCLUSIONI

Le minacce riportate nel corso della tesi sono solo la punta di un iceberg di un mondo in continua evoluzione, che ha impatti a livello globale e che può essere tanto utile quanto dannoso.

Le tecniche per monitorare e proteggere le reti aziendali sono infinite, in continuo incremento per cercare di limitare e contenere le nuove tecniche di evasione e attacchi informatici che i cybercriminali ogni giorno perpetuano nel mondo.

Come evidenziato nella prima parte del mio elaborato, le aziende vittime di attacchi informatici possono subire ingenti danni economici ed è per questo motivo che, anche nel panorama italiano, vengono rilasciati finanziamenti dallo Stato alle stesse, per permettere loro di implementare tecnologie all'avanguardia in grado di difenderle. La sola installazione di un EDR, ad esempio, permette già di avere una protezione efficace, sfruttando le conoscenze degli sviluppatori e dell'intelligenza artificiale dello strumento, senza la necessità di avere obbligatoriamente un SOC interno.

Durante il mio tirocinio presso l'azienda di cybersecurity HWG Srl, ho avuto l'opportunità di approfondire la mia conoscenza teorica acquisita durante il corso di laurea e di metterla in pratica in un contesto aziendale reale. Questa esperienza è stata estremamente formativa e mi ha offerto una

visione approfondita del campo della cybersecurity, permettendomi di comprendere appieno le sfide e le opportunità che questo settore in continua evoluzione presenta.

L'azienda ha dimostrato un alto livello di professionalità e competenza nel settore della cybersecurity. Ho avuto l'opportunità di lavorare a stretto contatto con professionisti esperti, che mi hanno guidato e supportato durante l'intero percorso del tirocinio, dandomi la possibilità di poter approfondire varie tecnologie e strumenti che vengono utilizzati quotidianamente.

Il tirocinio curricolare è un'esperienza utile e necessaria per permettere agli studenti di approcciarsi al mondo del lavoro ed avere delle prime applicazioni di materie viste solamente dal punto di vista teorico durante il percorso di studi. Tra i corsi da me frequentati, "Fondamenti di Informatica" e "Laboratorio di Programmazione" mi hanno permesso di gettare le basi di programmazione utili ad affrontare analisi di codici malevoli e poter gestire le automazioni che utilizzano alcuni EDR e SOAR. "Reti di Calcolatori" mi ha permesso di conoscere le nozioni fondamentali del modello ISO/OSI, utilizzato per definire le modalità con cui i dati vengono scambiati tra due macchine. Infine, il corso di "Secure Network Management And Computer Networks" mi ha fatto scoprire ed appassionare al mondo della cybersecurity, con nozioni teoriche sulle reti aziendali ma anche prove pratiche tramite laboratori virtuali.

Ritengo che l'opportunità di effettuare il tirocinio universitario presso HWG sia stata estremamente vantaggiosa per la mia formazione accademica e professionale in quanto mi ha permesso di acquisire competenze tecniche di alto livello nel campo della cybersecurity e di applicare le mie conoscenze teoriche in un ambiente aziendale dinamico. L'esperienza mi ha confermato l'importanza della continua formazione e aggiornamento nel campo dell'informatica, data la rapida evoluzione delle minacce e delle tecnologie. Grazie ad esso, inoltre, mi è stata data la possibilità di continuare il percorso lavorativo all'interno dell'azienda e di conseguire certificazioni per programmi utilizzati, in particolare quelle inerenti a Crowdstrike, prodotto nel quale mi sono potuto specializzare. Mi sono orientato verso questo strumento sin da subito in quanto colpito dalla sua efficacia, versatilità e immediatezza d'uso, pur avendo al contempo tra le mani, un tool che permette di effettuare analisi approfondite e risalire alla sorgente di attacchi informatici più complessi.

Consiglio vivamente ad altri studenti di considerare l'opportunità di effettuare un tirocinio curricolare, poiché rappresenta un'esperienza che arricchisce sia dal punto di vista professionale che personale e può offrire vantaggi agli studenti in termini di visibilità nel settore lavorativo, aspetto da non sottovalutare al giorno d'oggi.

SITOGRAFIA

- https://www.crowdstrike.com/it/
- https://www.hwg.it/
- https://www.cert.hu/sites/default/files/xforce_threat_intelligence_index_2021_90037390usen.pdf
- https://neinformatica.it/blog/privacy-e-sicurezza/gdpr-unopportunita-per-le-aziende/
- https://finanza.lastampa.it/News/2023/02/07/cybersecurity-+53percento-di-attacchi-informatici-negli-ultimi-4-anni/OTlfMjAyMy0wMi0wN19UTEI
- https://attack.mitre.org/techniques/T1055/
- https://attack.mitre.org/tactics/TA0003/
- https://www.openpolis.it/durante-la-pandemia-aumentano-gli-attacchi-informatici-in-ue/
- https://monokee.com/category/mfa/
- https://www.corrierecomunicazioni.it/digital-economy/boom-di-ransonware-nel-2021-riscatti-record-fino-a-50-milioni-usd/
- https://www.corriere.it/economia/aziende/20_dicembre_04/campari-sull-attacco-hacker-rubati-dati-4700-dipendenti-8dd83088-3645-11eb-ab19-bbfa6037f17b.shtml
- https://www.rainews.it/archivio-rainews/articoli/Attacco-hacker-al-sito-della-Siae-sottratti-60-gigabyte-di-dati-chiesto-un-riscatto-in-Bitcoin-2df88593-e421-46ef-85c4-5bc251e676e1.html
- https://www.redhotcyber.com/post/san-giovanni-addolorata-di-roma-la-timeline-dell-attacco-ransomware/
- https://www.csirt.gov.it/contenuti/attacchi-ddos-tipologie-e-azioni-di-mitigazione
- https://www.redhotcyber.com/post/rhc-rileva-4tb-di-dati-di-enel-in-vendita-nelle-underground-per-1000-euro-si-tratta-dellattacco-di-netwalker/
- https://www.cert.hu/sites/default/files/xforce_threat_intelligence_index_2021_90037390usen.pdf
- https://www.cybersecurity360.it/nuove-minacce/emotet-il-piu-pericoloso-framework-criminale-di-cyber-spionaggio-storia-evoluzione-e-tecniche-di-attacco/
- https://en.wikipedia.org/wiki/Zeus_(malware)
- https://www.secureworks.com/research/zeus
- https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/
- https://www.cybersecurity360.it/nuove-minacce/ransomware/mega-attacco-ransomware-mondiale-via-kaseya-perche-e-allarme-rosso/
- https://it.wikipedia.org/wiki/Accenture

- https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf
- https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
- https://www.crowdstrike.com/blog/tech-center/customizable-dashboards/
- https://www.crowdstrike.com/products/threat-intelligence/falcon-sandbox-malware-analysis/
- https://www.redhotcyber.com/post/accenture-timeline-dell-incidente-ransomware-lockbit-2-0/
- https://clusit.it/rapporto-clusit/
- https://www.cybersecurity360.it/soluzioni-aziendali/siem-cos-e-come-garantisce-la-sicurezza-delle-informazioni/
- https://it.wikipedia.org/wiki/Protocollo_Kerberos
- https://it.wikipedia.org/wiki/Indicatore_di_compromissione
- https://it.wikipedia.org/wiki/Active_Directory
- https://it.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
- https://en.wikipedia.org/wiki/Deep_packet_inspection
- https://www.ibm.com/it-it/topics/siem
- https://en.wikipedia.org/wiki/Endpoint_detection_and_response
- https://en.wikipedia.org/wiki/CrowdStrike
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/
- https://www.repubblica.it/cronaca/2017/12/08/news/cybercrimine_blitz_polizia-fbi_contro_hacker_della_rete_andromeda_-183462911/
- https://www.ansa.it/europa/notizie/europarlamento/news/2022/11/23/cyberattacco-al-sito-del-parlamento-europeo-servizi-compromessi_961b642b-4dfa-4971-b8b6-8741ec375b11.html
- https://www.ilsole24ore.com/art/cybersecurity-mercato-balza-19-miliardi-italia-AEiqjkrC
- https://www.cybersecurity360.it/outlook/pnrr-e-cyber-security-la-vera-sfida-e-investire-meglio/
- https://www.tomshw.it/business/crowdstrike-la-sicurezza-it-interamente-in-cloud-per-sistemi-agili/
- https://www.airlockdigital.com/airlock-v4-5-released-linux-enforcement-agent-crowdstrike-integration-rbac-etc/

- https://openapi.it/blog/cosa-e-chiamata-api.html