Ransomware

Vantaggi chiave

- La tecnologia Cyber AI di self-learning neutralizza i ransomware emergenti, senza fare affidamento a regole o segni distintivi di minacce
- L'Enterprise Immune System è in grado di identificare anche le specie di ransomware nuove e altamente mirate
- Antigena risponde autonomamente in tempo reale, indipendentemente da dove, quando o come viene lanciato l'attacco
- Il Cyber AI Analyst indaga automaticamente sugli incidenti ransomware, riunendo tutte le principali informazioni necessarie a mettere in pratica una remediation

Figura 1: La Cyber AI identifica un attacco ransomware

Lo scorso anno i ransomware hanno causato perdite per un totale di 381 milioni di dollari a danno di 350 aziende

Fonte: Hiscox, 2020

Poiché le regole e innovazioni tecniche che riguardano la forza lavoro di oggi sono in rapida evoluzione, gli attacchi ransomware sono sempre più sofisticati e diffusi.

Stanno emergendo nuove specie di ransomware che sfruttano malware senza file e tattiche di esfiltrazione di dati, mentre i pirati informatici più opportunistici sfruttano qualsiasi mutamento delle circostanze per lanciare campagne ancora più efficaci. Gli strumenti di sicurezza convenzionali, che rilevano solo le minacce informatiche conosciute utilizzando regole e firme, non sono in grado di individuare le specie evolute di ransomware per le quali queste firme non esistono.

I team della sicurezza non sono in grado di rimanere al passo di queste minacce utilizzando solo i controlli tradizionali, soprattutto quando sono a corto di personale o fuori ufficio. Al contrario, le aziende devono adottare tecnologie per la sicurezza in grado di bloccare i ransomware non appena emergono, prima che possano causare danni.

Cyber AI Platform di Darktrace: identificazione e risposta a ransomware emergenti

La Cyber AI Platform di Darktrace è in grado di neutralizzare significativamente e in tempo reale ransomware avanzati, senza fare affidamento su intelligenza o firme di minacce conosciute. Basandosi sul machine learning non supervisionato e su tecniche di apprendimento dettagliato, la Cyber AI apprende i normali "pattern of life" di ogni utente e tecnologia all'interno dell'organizzazione per riconoscere le impercettibili deviazioni che identificano una minaccia emergente.

L'Enterprise Immune System utilizza la conoscenza in continua evoluzione che la Cyber AI ha di "sé" all'interno del contesto aziendale per individuare qualsiasi minaccia informatica, inclusi ransomware mai visti prima che eludono tutte le altre strategie difensive. Il Cyber AI Analyst, elemento fondamentale dell'approccio basato sul sistema immunitario, indaga in modo automatico su qualsiasi minaccia, consentendo di identificare facilmente qualsiasi dispositivo compromesso e comunicando l'ambito completo di un incidente ransomware.

Non appena viene segnalato un attacco grave, Darktrace Antigena, la tecnologia di Autonomous Response della piattaforma, è in grado di arginare in pochissimi secondi l'attività pericolosa, neutralizzando chirurgicamente gli attacchi e consentendo nel contempo il normale svolgimento delle attività aziendali. La tecnologia è in grado di adattarsi intelligentemente alle minacce non appena vengono individuate, fornendo una copertura 24 ore su 24, 7 giorni su 7 quando i team della sicurezza sono sovraccarichi o semplicemente non disponibili.

La resilienza alla velocità delle macchine è fondamentale per minimizzare l'impatto di un ransomware, che spesso è in grado di crittografare in pochi minuti l'infrastruttura di un'azienda. Inoltre, la Cyber AI Platform è in grado di correlare in modo esclusivo i pattern all'interno di tutta l'attività aziendale, fornendo una visione e un controllo unificati anche quando gli attacchi ransomware colpiscono diverse parti dell'ecosistema digitale: dalle e-mail alle piattaforme SaaS, dalle reti aziendali ai sistemi industriali.

Antigena Network: neutralizzare gli attacchi alla velocità delle macchine

Quando un ransomware emerge, Antigena Network è l'unica soluzione in grado di bloccare l'attacco alla velocità delle macchine e con precisione chirurgica, anche quando la minaccia è mirata o totalmente sconosciuta. Risponde in modo autonomo con azioni intelligenti e proporzionate, ad esempio interrompendo una connessione o forzando il normale "pattern of life" di uno specifico dispositivo. Quando il team della sicurezza è sovraccarico o non disponibile, Antigena Network fornisce la sicurezza di sapere che l'intera azienda è sempre protetta, 24 ore su 24, 7 giorni su 7.

Darktrace ha creato la tecnologia di Autonomous Response di Antigena, che utilizza la conoscenza in continua evoluzione che la Cyber AI ha sull'intera organizzazione per adattarsi alle minacce in tempo reale e adottare le soluzioni più appropriate in base al contesto specifico. Anziché applicare un blocco binario (ad es. mettendo completamente in quarantena il dispositivo) come farebbe uno strumento tradizionale, Antigena agisce in modo chirurgico per bloccare l'attacco, garantendo la continuazione della normale operatività aziendale. La tecnologia è anche in grado di integrarsi con le tecnologie di sicurezza esistenti per ampliare così lo stack di sicurezza, fornendo a firewall, SIEM e ad altri strumenti informazioni e azioni guidate dall'AI.

Interruzione del ransomware Ryuk durante la prova di Darktrace

Quando il ransomware Ryuk ha colpito un'azienda che aveva installato Darktrace in prova, l'Enterprise Immune System lo ha rilevato istantaneamente e ha indicato come Antigena Network avrebbe potuto bloccarlo completamente.

Per prima cosa, la Cyber AI ha notato un'attività dell'amministratore estremamente insolita mai vista in precedenza sulla rete. A seguito dell'incidente, l'azienda ha tracciato la compromissione iniziale in una parte della propria rete sulla quale Darktrace non aveva visibilità durante il periodo di prova.

La Cyber AI ha quindi rilevato che il famigerato trojan bancario TrickBot era stato scaricato, in seguito al rilevamento di comando e controllo del traffico. Anche se molti dispositivi avevano un comportamento anomalo, la Cyber AI ha localizzato con precisione un dispositivo come origine.

Quando il ransomware Ryuk è stato infine installato, in sole 12 ore erano stati crittografati più di 200.000 file. Durante questo periodo "confuso" con molte attività SMB sospette, la Cyber AI aveva indicato ancora più chiaramente l'estensione dell'attacco.

Anche se il team aveva messo in pratica gli allarmi di Darktrace solo dopo la crittografia, questo attacco ransomware avrebbe potuto essere fermato non appena l'Enterprise Immune System aveva rilevato i primi segnali di compromissione.

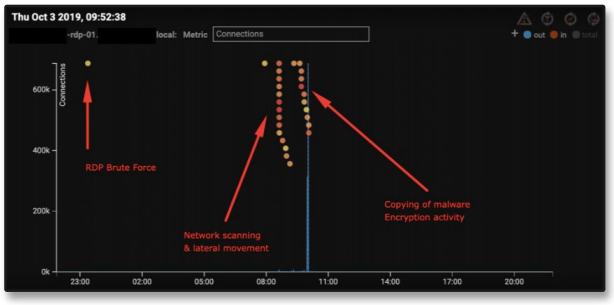

Figura 2: Il grafico UI mostra un esempio di attacco ransomware; ogni punto rappresenta un allarme di Darktrace.

Autonomous Response in pochi secondi

Se l'azienda avesse impiegato la tecnologia di Autonomous Response di Antigena Network, la mancata attenzione verso gli allarmi attivati da Darktrace non avrebbe causato alcun problema: anche se erano passate quattro ore da quando il primo file crittografato era stato scaricato, Antigena avrebbe neutralizzato la minaccia in pochi secondi. Le azioni che Antigena avrebbe messo in atto in risposta ad alcuni degli allarmi relativi a questo incidente includono:

- **Sessione SMB Admin insolita:** credenziali compromesse utilizzate per accedere al server
  - **Risposta di Antigena:** questa singola anomalia non attiva alcuna azione, ma aumenta il livello di allerta
- **Nuove credenziali Admin sul client:** il pirata informatico ha utilizzato numerose nuove credenziali amministratore sul dispositivo
  - **Risposta di Antigena:** ora, grazie ad una maggiore certezza sull'evidenza di una minaccia, Antigena avrebbe forzato i tipici "pattern of life" di accesso del dispositivo; tutti gli amministratori che normalmente accedono a questo dispositivo possono continuare a farlo, mentre i nuovi accessi sono bloccati per un'ora.
- **Scansione della rete:** il pirata informatico aveva eseguito una scansione della rete per identificare ulteriori vittime
  - **Risposta di Antigena:** questo server non aveva mai eseguito in precedenza una scansione della rete; solo i dispositivi amministratore lo fanno. Antigena pertanto avrebbe bloccato per due ore la scansione della rete da parte del dispositivo.
- **EXE da una sede esterna rara:** payload scaricati in fase successiva per un'ulteriore infezione
  - **Risposta di Antigena:** Antigena avrebbe consentito al dispositivo di continuare i normali download bloccando nel contempo quelli da posizioni rare.

Antigena Email: fermare i ransomware all'origine

Molti attacchi ransomware hanno origine dalle piattaforme di posta elettronica, dimostrando che i gateway tradizionali delle email e gli approcci legacy che si basano su regole e firme non sono abbastanza efficaci da rilevare di volta in volta ransomware evoluti. Inoltre, queste soluzioni tradizionali hanno un ambito limitato e non sono in grado di correlare le attività di posta elettronica alle azioni pericolose all'interno dell'infrastruttura digitale.

Grazie all'efficacia della Cyber AI, Antigena Email è in grado di creare una comprensione estesa su ogni singolo essere umano che si cela dietro ad un indirizzo e-mail. La tecnologia si adatta alla dinamicità di ogni forza lavoro in modo da riconoscere anche le sfumature più significative nei comportamenti che identificano una campagna ransomware in corso.

La tecnologia risponde quindi in modo autonomo e proporzionato per bloccare la minaccia alla velocità delle macchine e proteggere l'organizzazione contro qualsiasi vulnerabilità, bloccando completamente l'e-mail, un link o convertendo gli allegati in un tipo di file innocuo.

Se il ransomware superasse la casella di posta in arrivo e accedesse alla rete, Antigena Email è in grado in modo unico di sfruttare l'Enterprise Immune System per tracciare l'origine dell'attacco e prevenire la diffusione laterale.

Correlando i pattern delle attività del resto del contesto aziendale con l'ambiente di posta elettronica, la Cyber AI è in grado di eseguire un'analisi della causa principale per identificare l'e-mail origine e altre attività di posta elettronica che possono essere correlate all'incidente. Antigena Email è in grado poi di recuperare qualsiasi altra e-mail pericolosa dalle caselle di posta in arrivo degli altri dipendenti, minimizzando quindi l'estensione dell'attacco ransomware.

Entro il 2021 ci sarà un attacco ransomware ogni 11 secondi.

Fonte: Cybersecurity Ventures

Figura 3: Antigena Email rileva una serie di e-mail associate alla campagna ransomware

Link pericolosi neutralizzati presso un'Amministrazione comunale

Un'amministrazione comunale molto nota negli Stati Uniti è stata recentemente vittima di un'attacco mirato che aveva origine dalle e-mail, con il tentativo di distribuire un ransomware all'interno dell'organizzazione. Fortunatamente Antigena Email ha rilevato la minaccia non appena si è presentata, assicurandosi che nessun payload, ransomware o altro elemento pericoloso potesse essere scaricato.

Sembrava che il pirata informatico avesse accesso alla rubrica degli indirizzi dell'amministrazione comunale, poiché ogni e-mail era stata appositamente creata e personalizzata per il destinatario e inviata in ordine alfabetico, dalla A alla Z. Anche se ogni e-mail sembrava non pericolosa, tutti i messaggi contenevano un payload pericoloso nascosto dietro ad un pulsante camuffato in modo diverso, come un link a Netflix, Amazon e altri servizi affidabili.

Antigena Email è riuscita ad analizzare questi link nascosti in associazione con i normali "pattern of life" dei destinatari previsti. Quando la prima e-mail è stata recapitata, Antigena ha riconosciuto immediatamente che né il destinatario né nessun altro nel suo gruppo di colleghi o altri membri dello staff dell'amministrazione comunale avevano mai visitato il dominio del mittente.

La tecnologia ha generato istantaneamente un allarme di alta priorità e ha suggerito autonomamente il blocco di ciascun link non appena entrava nella rete.

Poiché Antigena era stata installata in "modalità passiva", non era in grado di agire in modo indipendente per fermare la minaccia alla velocità delle macchine, ma ha dimostrato l'efficacia della Cyber AI e dell'Autonomous Response. Mentre Antigena ha individuato e richiesto di neutralizzare la minaccia già alla lettera "A", gli strumenti esistenti del team della sicurezza sono entrati in azione solo alla lettera "R".

In "modalità attiva", Antigena avrebbe neutralizzato l'attacco prima che potesse raggiungere anche solo un utente, difendendo questa importante organizzazione dalla potenziale diffusione di un attacco ransomware.

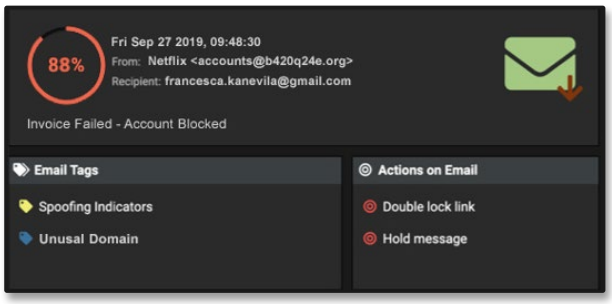

Figura 4: Antigena Email segnala che ogni e-mail è estremamente anomala.

Tracciatura da parte di un ransomware di un account e-mail personale

Non appena un ransomware è stato recapitato nella casella di posta in arrivo di una grande azienda di telecomunicazioni, la Cyber AI Platform di Darktrace è stata in grado di rilevare e contenere in modo autonomo l'attacco prima che potesse crittografare anche un solo file.

La compromissione iniziale si è verificata quando un dipendente ha acceduto alla sua e-mail personale da uno smartphone aziendale e, dopo essere stato ingannato, ha scaricato un file dannoso, contenente un ransomware. Alcuni secondi dopo, il dispositivo ha iniziato a collegarsi ad un server esterno sulla rete Tor e sono iniziate attività di crittografia SMB.

In soli nove secondi, la Cyber AI ha attivato un allarme prioritario indicando la necessità di un'indagine immediata sul comportamento raro.

Visto che il comportamento persisteva nei pochi secondi successivi, la Cyber AI ha modificato la propria decisione e Antigena ha risposto in modo autonomo.

Dato che il team addetto alla sicurezza era andato a casa per il week-end, Antigena Network ha bloccato autonomamente l'attacco, interrompendo tutti i tentativi di allegare i file crittografati nelle condivisioni di rete.

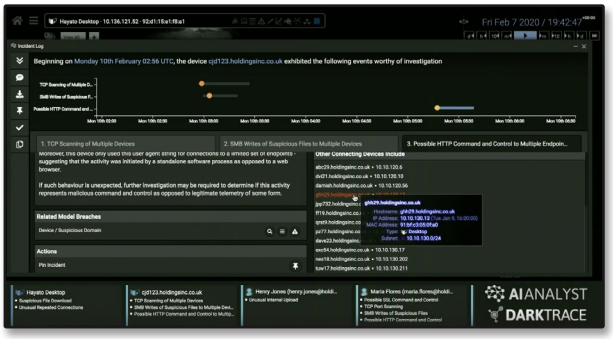

Figura 5: L'immagine campione UI mostra la Cyber AI che segnala attività SMB anomale simili.

Se l'azienda avesse installato Antigena Email, è molto probabile che il ransomware non sarebbe nemmeno stato scaricato. Nessuno strumento è una soluzione ottimale, ma anche se il ransomware avesse acceduto alla rete attraverso la casella di posta elettronica, Antigena Email avrebbe correlato l'attività pericolosa rilevata nella rete con l'e-mail compromessa in origine. La tecnologia avrebbe poi recuperato altre e-mail pericolose simili da tutto il traffico email aziendale.

Solo attraverso una comprensione dettagliata e in continua evoluzione del DNA dell'organizzazione, Antigena Email e l'intera Cyber AI Platform di Darktrace sono in grado di offrire questo rilevamento in tempo reale e rispondere ad attacchi ransomware sofisticati.

Enterprise Immune System con Cyber AI Analyst: comprensione dell'ambito completo di un incidente ransomware

Il self-learning della Cyber AI consente all'Enterprise Immune System di rilevare qualsiasi sfumatura di cambiamento nelle attività che indica la presenza di un ransomware, senza fare affidamento sull'intelligenza di una minaccia conosciuta. Grazie alla comprensione personalizzata e in continua evoluzione dei normali "pattern of life"all'interno di un'infrastruttura, l'Enterprise Immune System identifica anche le deviazioni più impercettibili, informando il team della sicurezza della presenza di un attacco alla velocità delle macchine.

Il Cyber AI Analyst, componente fondamentale dell'approccio basato sul sistema immunitario, indaga automaticamente qualsiasi evento anomalo rilevato. In caso di campagne ransomware, è in grado di identificare qualsiasi dispositivo interessato, l'origine dell'infezione e di fornire le informazioni contestuali necessarie ad attivare una risposta.

Il Cyber AI Analyst ha dimostrato di ridurre il tempo di investigazione del 92% ed è in grado di evidenziare abilmente ransomware emergenti come una minaccia di livello critico che richiede una valutazione umana. Un "Incident Report" generato dall'AI offre una cronologia degli eventi interattiva, un riepilogo conciso sulla campagna, nonché dati granulari sui comportamenti di utenti o dispositivi correlati.

Questi report si aggiornano autonomamente mentre la minaccia si evolve e sono fondamentali nell'aiutare gli esperti della sicurezza ad ottenere una consapevolezza sulla situazione, nonché per la condivisione di informazioni importanti anche con gli stakeholder non tecnici.

Analisi esperta di un attacco Dharma

Quando è stata lanciata una campagna ransomware Dharma mirata ad un'azienda nel Regno Unito, l'Enterprise Immune System è stato fondamentale nel rilevare questa minaccia, mostrando anche l'efficace capacità del Cyber AI Analyst nel riconoscere e segnalare un attacco emergente.

La Cyber AI ha individuato istantaneamente il rischio non appena un server RDP ha ricevuto un gran numero di connessioni da indirizzi IP rari. Un'indagine successiva ha rivelato che le credenziali RDP erano state probabilmente compromesse in un momento impreciso prima dell'attacco.

Il giorno dopo, la Cyber AI ha individuato il tentativo da parte del pirata informatico di abusare del protocollo SMB versione 1. Successivamente, sono state individuate un'insolita connessione esterna ad un raro indirizzo IP marocchino e una sessione SMB non riuscita dell'IP su una porta estremamente insolita. Due ore dopo, il pirata informatico ha creato canali di comando e controllo più efficaci, effettuando collegamenti a destinazioni rare in India, Cina e Italia.

La Cyber AI ha individuato anche una ricognizione interna quando connessioni RDP in ingresso hanno iniziato ad effettuare la scansione della rete e un grande volume di dati è stato trasferito ad un indirizzo IP insolito a Panama.

Infine, è stato eseguito il payload Dharma. Parallelamente all'attività di crittografia, il ransomware ha tentato di infettare altre macchine utilizzando le credenziali di amministratore individuate durante la ricognizione interna. Quando è iniziata la crittografia, lo staff IT ha staccato la spina dal server RDP.

Anche se in precedenza il team aveva trascurato gli avvisi di azione di Darktrace, la Cyber AI è stata comunque in grado di riconoscere ogni passaggio di questo attacco evoluto, consentendo al team di rispondere efficacemente e prevenire ulteriori danni.

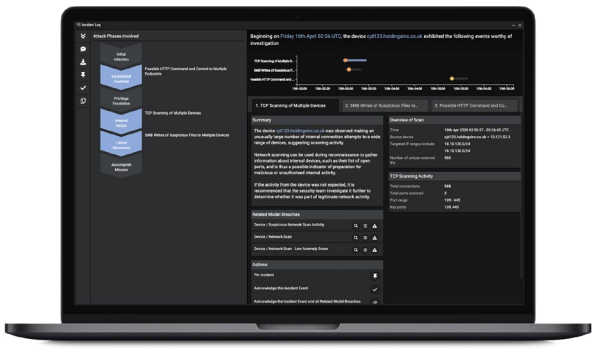

Figura 6: L'immagine campione UI mostra il Cyber AI Analyst che segnala un attacco ransomware.

L'Enterprise Immune System ha individuato ogni fase di questa campagna, basandosi sui comportamenti anomali all'interno del contesto aziendale, senza dipendere dal riconoscimento di firme di minacce note.

Quando si ha a che fare con un attacco di questo tipo, che si sviluppa nel corso di un lungo periodo di tempo e con indicatori eterogenei di attività pericolose, il Cyber AI Analyst è fondamentale per mostrare chiaramente la natura e l'estensione della minaccia.

Grazie all'Incident Report del Cyber AI Analyst, il team può facilmente analizzare sia un riepilogo ad alto livello dell'attacco ransomware che i dettagli granulari di ogni fase dell'incidente.

Industrial Immune System: difesa dei sistemi operativi contro i ransomware

Quando si parla di difesa contro i ransomware, l'Industrial Immune System è la soluzione più efficace per gli ambienti di sicurezza operativa moderni. Soprattutto di fronte a minacce come il ransomware EKANS, il primo ransomware noto per prendere di mira infrastrutture ICS specifiche, è fondamentale sfruttare strumenti di sicurezza in grado di adattarsi continuamente agli ambienti OT e di difendere questi sistemi anche contro attacchi zero-day.

Molte campagne ransomware prendono di mira anche ambienti industriali attraverso vulnerabilità presenti nelle infrastrutture IT. Le compromissioni indirette costituiscono anche un'ulteriore minaccia, poiché i sistemi OT possono diventare un danno collaterale durante attacchi mirati all'IT. Data la potenziale minaccia all'infrastruttura critica, la necessità di una tecnologia di sicurezza in grado di correlare pattern all'interno di infrastrutture eterogenee è sempre più urgente.

L'AI di self-learning consente all'Industrial Immune System di identificare chiaramente le minacce anche più evolute come nuovi ransomware. La tecnologia è in grado di apprendere i normali "pattern of life" per tecnologie e tipologie di deployment radicalmente differenti, da PLC molto obsoleti a sensori distribuiti, all'IoT industriale.

Inoltre, grazie alla sua visione unificata, la Cyber AI comprende il collegamento tra attività pericolose nei sistemi IT e i comportamenti nei sistemi OT, rendendola chiaramente capace di bloccare le minacce mentre si spostano all'interno di ciò che è tradizionalmente messo in sicurezza in modo statico.

Scoperta di un ransomware presso una raffineria petrolifera

Presso un impianto integrato di raffinazione e fornitura di petrolio, l'Industrial Immune System di Darktrace è stato fondamentale nel bloccare un attacco ransomware che aveva avuto origine nella rete aziendale.

La Cyber AI ha identificato i primi segnali di un'infezione ransomware in un dispositivo desktop collegato in rete. Anche se stava scrivendo il proprio file di note ransom, è stato rilevato che il dispositivo stava eseguendo una serie di connessioni verso destinazioni esterne rare tramite un server proxy interno, scaricando poi file potenzialmente pericolosi, attività che Darktrace è stata in grado di rilevare e correlare in base alla sua conoscenza granulare del "sé" dell'azienda.

Il dispositivo eseguiva una serie di query directory SMB, ulteriore attività che la Cyber AI ha riconosciuto come anomala sulla base della sua conoscenza di quel particolare dispositivo.

L'Industrial Immune System ha segnalato questa attività, indicandola come un probabile ransomware, avvisando il team della sicurezza del cliente prima che l'infezione fosse in grado di diffondersi negli ambienti OT.

Grazie alla capacità che la Cyber AI ha di collegare i pattern all'interno di infrastrutture diverse, è stato possibile difendere questo sistema industriale da un attacco alla velocità delle macchine.

Figura 7: L'immagine UI campione mostra un dispositivo infetto con un ransomware identificato dalla Cyber AI.