Risposta della cyber IA: Report sulle minacce 2019

Introduzione

I business leader dell'era digitale affrontano fattori di rischio estremamente urgenti in un'epoca di minacce informatiche automatizzate e rapide. Questi rischi sono aumentati notevolmente negli ultimi anni poiché le minacce si sviluppano e diventano sempre più avanzate e i nostri business digitali continuano a crescere in termini di complessità, diversità e portata.

In passato, quando gli actor di minacce erano meno avanzati e quando le reti erano più prevedibili, un approccio tradizionale alla sicurezza era spesso adeguato per controllare le minacce informatiche. Configurando strumenti di sicurezza con qualche combinazione di regole o firme, i team addetti alla sicurezza hanno cercato di rilevare le minacce definendole in anticipo "benigne" o "dannose", affidandosi alle descrizioni di attacchi che sono stati concepiti sotto forma di regola o che sono stati osservati "allo stato brado" e sottoposti a reverse-engineering per il rilevamento futuro.

E ancora, la maggiore frequenza di nuovi attacchi esterni e di minacce interne, unita alla complessità e alla precarietà dei comportamenti di tutti i giorni in un'attività commerciale, ha gradualmente disarmato i team addetti alla sicurezza che si affidano ancora ai controlli tradizionali. Le difese tradizionali non riescono a rilevare le nuove tattiche e tecniche dei sofisticati pirati informatici, che ora possono penetrare nel caos della rete e diffondersi nelle infrastrutture ampie e complesse in pochi secondi.

Il fatto è che le nuove minacce si insidieranno inevitabilmente, quindi l'attenzione del settore si è spostata sulla richiesta di cosa possono fare i difensori informatici per rilevare e rispondere alle minacce emergenti che sono già all'interno del business, ma che possono essere gestite prima che si trasformino in crisi. I business leader e i team addetti alla sicurezza si sono rivolti all'intelligenza artificiale per non rimanere indietro.

L'esclusiva applicazione di IA di Darktrace apprende invece il normale "pattern of life" per le singole aziende e individua sottili deviazioni che indicano una minaccia, sia essa nota o sconosciuta, esterna o interna, celata o veloce. Imparando "sul campo" e adattandosi continuamente alle nuove evidenze, l'intelligenza artificiale di Darktrace individua i primi indicatori di minacce informatiche che, diversamente, passerebbero inosservati, senza affidarsi a regole, firme o precedenti supposizioni.

Riepilogo

Questo report illustra dettagliatamente sette case study di attacchi che sono stati intercettati e neutralizzati grazie all'IA per la cyber defense, compresi minacce interne, ransomware e attacchi IoT.

Anche se tutti gli scenari di minaccia erano ben distinti, alcuni rapidi e altri lenti e furtivi, in tutti i casi gli indicatori celati di attività sospetta erano rilevabili solamente usando l'IA Darktrace, che impara ciò che è normale per l'infrastruttura dell'azienda e risponde agli attacchi in modo del tutto autonomo, prima che il danno sia completato.

Contrattacco con Darktrace Antigena

Poiché il gap delle competenze si allarga e il volume e la velocità degli attacchi aumentano, l'IA non è più solamente fondamentale nel rilevare le minacce emergenti, ma ci si affida ad essa anche per rinforzare la risposta di prima linea dell'organizzazione. Questa è un'IA in grado di contrattaccare in tempo reale, dando al team addetto alla sicurezza il tempo per riprendersi.

Grazie alla sua ricca e mutevole comprensione del normale "pattern of life" per ciascun utente, dispositivo e gruppo di simili associato in un'azienda, l'IA di Darktrace non solo riesce a rispondere ai primi indicatori di minaccia informatica prima che facciano danni, ma lo fa anche in un modo altamente mirato. Anziché generare quarantene applicate in modo esteso che causerebbero solamente altre interruzioni, Darktrace Antigena, la soluzione di risposta di IA informatica del sistema, lavora applicando chirurgicamente il normale "pattern of life" per un dispositivo infetto o un dipendente che aveva subito un attacco informatico, neutralizzando la minaccia entro pochi secondi e sostenendo le normali operazioni con il design.

Nella lotta contro pirati informatici progrediti, l'IA informatica di Darktrace ripristina il controllo ai difensori, trasformando persino l'organizzazione più complessa e vulnerabile in un digital business resistente e in grado di difendersi.

Minaccia interna

Un dipendente analizza la rete per rilevarne i punti deboli

Dannosa e persistente

La minaccia interna è uno dei vettori di attacco più pericolosi e comuni all'interno di un'azienda, sia essa dannosa oppure no. Insider dannosi rappresentano una minaccia particolarmente significativa per l'azienda, poiché il loro accesso privilegiato e le loro conoscenze della rete consentono di intraprendere missioni di attacco piuttosto estese ed esfiltrarsi in tutta tranquillità o manipolare dati fondamentali senza destare sospetti.

L'IA di Darktrace ha individuato e neutralizzato questo tipo di insider dannoso in un'importante azienda di investimenti in Sudafrica. L'IA di auto-apprendimento è riuscita a contenere una minaccia persistente, spostandosi attraverso più fasi della catena di attacco, dal riconoscimento alla scrittura e all'esecuzione degli script. Imparando "sul campo", Antigena si è adattato alla minaccia durante la sua evoluzione e l'ha contenuta in modo efficace in ogni fase.

Comportamento sospetto

La fase di riconoscimento è iniziata con un laptop che "eseguiva un ping" con centinaia di indirizzi IP interni per identificare quelli attivi. Dopodiché, ha ripulito la rete per cercare i nomi delle macchine che rispondevano e le ha analizzate per individuare canali di comunicazione aperti. L'IA di Darktrace ha segnalato il comportamento sospetto come attività insolita di scansione della rete e ha indicato immediatamente ad Antigena di intervenire. In base alla sua valutazione dinamica della minaccia, Antigena ha deciso di rafforzare il "pattern of life" del gruppo del dispositivo per un'ora, impedendo al laptop di deviare dal suo comportamento precedente o da quello dei suoi simili.

Qualche ora dopo, la minaccia è tornata. Il laptop ha iniziato ad eseguire dei comandi su centinaia di altri computer interni nell'intervallo IP inizialmente identificato. Erano compresi lo spostamento di file di script multiuso e l'uso di uno strumento di amministrazione remota. Questi programmi potevano essere usati per individuare informazioni sensibili e documenti importanti o per aprire una backdoor per un pirata informatico esterno per furti futuri.

> Antigena ha deciso di applicare il "pattern of life" di gruppo del dispositivo per un'ora

Intervento di Antigena

Durante questo periodo di tempo nessun'altra scrittura di file simile è stata individuata sulla rete, comportamento rilevato come altamente insolito per l'IA di Darktrace. Data la sua mutevole comprensione della minaccia nel contesto della rete e la sua precedente risposta autonoma, Antigena ha deciso di bloccare tutte le connessioni in uscita che utilizzavano il canale di trasferimento file SMB, contenendo immediatamente tutti gli spostamenti laterali attraverso la rete.

Una volta che la minaccia è stata neutralizzata, il team addetto alla sicurezza è riuscito a indagare e a confermare che il laptop apparteneva ad un membro del team IT che stava utilizzando uno strumento di scansione illegale per cercare i punti deboli nella rete. Questo è un esempio particolarmente eloquente del potere dell'IA di Darktrace e di come Antigena riesca a intervenire in diverse fasi di una catena di attacco e a neutralizzare le minacce persistenti nella loro fase iniziale.

Trojan zero-day

Download e connessioni sospette

Una nuova specie di malware

Anche se gli strumenti di sicurezza esistenti riescono spesso a identificare le minacce note che sono già state scoperte, l'IA riesce ad individuare in modo esclusivo i segnali deboli e celati di una minaccia informatica mai vista prima. Questa capacità è diventata necessaria negli ultimi anni, poiché i pirati informatici progrediti continuano a sviluppare nuove tattiche, tecniche e procedure appositamente studiate per eludere i controlli che sono stati pre-programmati con le firme degli attacchi passati.

La capacità di Darktrace di reagire a questi indicatori celati è stata fondamentale per un produttore americano di controlli IoT industriali, quando è stato colpito da un trojan zero-day.

Alle 13:30 di un giovedì, l'IA ha avvisato il responsabile IT dell'azienda in merito a un download sospetto di un file denominato "OfficeActive.bin". Anche se il file sembrava un prodotto Microsoft, Darktrace ha indicato che il file veniva scaricato da una fonte non identificata che era al 100% rara per la rete.

> Anche se il file sembrava un prodotto Microsoft, Darktrace ha indicato che il file veniva scaricato da una fonte non identificata

Creare fiducia nella risposta dell'IA

In quel momento Antigena è stato configurato in "Modalità passiva", una modalità iniziale che limita l'IA alla comunicazione di ciò che avrebbe fatto in risposta alla minaccia, senza intervenire effettivamente, consentendo al team di creare fiducia nel processo di decision-making del sistema. Il team IT è riuscito a vedere in che modo Antigena avrebbe fermato l'attacco nella fase iniziale, e persino come si sarebbe adattato ad una nuova minaccia alla sua intensificazione.

In risposta al pattern di attività altamente insolito, Antigena ha consigliato prima di applicare il "pattern of life" di gruppo del dispositivo per due ore, cosa che avrebbe fermato la minaccia nei suoi percorsi, sostenendo contemporaneamente le normali operazioni.

Non appena ha osservato altri download sospetti, Antigena ha intensificato la sua risposta, applicando il "pattern of life" singolo del dispositivo per cinque minuti. Quando il dispositivo ha tentato di creare una nuova connessione esterna, Antigena ha di nuovo risposto, suggerendo che l'IA bloccasse chirurgicamente tutte le connessioni in uscita dal dispositivo per un'ora.

Risolvere la minaccia

Entro pochi minuti dall'identificazione dell'allarme, il responsabile IT ha contattato l'utente finale e ha eseguito una ricomposizione di emergenza per risolvere la minaccia sulla macchina. L'intero processo è stato completato entro 20 minuti. Una volta che la minaccia è stata neutralizzata, il responsabile IT ha copiato l'URL del trojan e il nome del file in Virus Total per controllare se la minaccia era stata osservata e registrata da qualche parte. La ricerca non ha dato risultati, confermando che si è trattato di un trojan zero-day scoperto eccezionalmente dall'IA di Darktrace.

IoT Hack: TVCC

Spionaggio aziendale?

Videocamera di sicurezza compromessa

La crescente connettività dei dispositivi di tutti i giorni ha introdotto ancora più vulnerabilità nel mondo dell'impresa. I dispositivi IoT, spesso progettati con controlli di sicurezza base non integrati, sono regolarmente bersaglio degli actor di minacce e vengono usati come trampolino per entrare nella rete.

In un'attività di consulenza per gli investimenti giapponese, Darktrace ha scoperto che in un sistema TVCC collegato ad Internet si erano infiltrati dei pirati informatici sconosciuti. Gli esecutori erano riusciti ad avere un punto d'appoggio nella rete e potevano guardare tutte le registrazioni effettuate con la videocamera. Installata per monitorare tutta l'area degli uffici, dall'ufficio del CEO alla sala riunioni, la videocamera stessa era così diventata un rischio per la sicurezza.

> L'IA ha contrattaccato alla velocità della macchina, impedendo una grave violazione

Reazione rapida

L'IA di Darktrace ha rilevato rapidamente che c'era qualcosa di strano. Grandi volumi di dati venivano osservati mentre si spostavano avanti e indietro dal server TVCC decrittografato, quando il pirata informatico ha raccolto i dati per poi esfiltrare informazioni sensibili.

Nel momento in cui il pirata informatico ha cercato di esfiltrare i dati, Antigena è intervenuto con un'azione difensiva rapida e precisa. Il sistema ha deciso di bloccare chirurgicamente lo spostamento dei dati dal dispositivo ad un server esterno, consentendo al sistema TVCC di continuare a funzionare come previsto.

L'IA ha contrattaccato alla velocità della macchina, impedendo una grave violazione delle informazioni di mercato sensibili. Intervenendo in modo proporzionato per contenere l'attacco nella sua fase iniziale, Antigena ha dato al team addetto alla sicurezza il tempo vitale per indagare e fermare la minaccia prima che causasse danni.

IoT Hack: smart locker

Obiettivo: dati sensibili dei clienti

Vulnerabilità IoT

In un parco divertimenti del Nord America, un actor di minacce ha tentato di rubare dati sensibili sui clienti tramite un dispositivo IoT vulnerabile: uno "smart" locker usato dai visitatori per conservare effetti personali.

Come parte delle sue impostazioni predefinite, lo smart locker stabiliva regolarmente il contatto con la piattaforma online di terze parti del fornitore. L'actor di minacce ha individuato la fonte di questo processo automatizzato e ne ha assunto il controllo per compromettere il dispositivo.

Profilo basso e lento

L'IA di Darktrace ha individuato l'attacco poco dopo che il locker ha iniziato a inviare una quantità insolita di dati decrittografati ad un sito esterno raro. Le connessioni erano temporizzate in base alle comunicazioni regolari del dispositivo con la piattaforma del fornitore, suggerendo che si trattava di un attacco "a profilo basso e lento", appositamente studiato per evadere i sistemi di difesa della sicurezza basati sulle regole.

Analizzando continuamente le comunicazioni in relazione al precedente comportamento del locker e quello dei suoi simili, l'IA di Darktrace ha determinato che era necessaria una risposta informatica dell'IA. In pochi secondi, Darktrace Antigena è entrato in azione, bloccando in modo intelligente tutte le connessioni in uscita dal dispositivo compromesso, dando al team addetto alla sicurezza il tempo di fermare la minaccia e impedire ulteriori esfiltrazioni.

Per questo e per altri parchi divertimenti, l'IA informatica di Darktrace ha neutralizzato gli infiniti attacchi "a profilo basso e lento" nella loro fase iniziale. Imparando "sul campo", il sistema individua le minacce celate che altri strumenti non rilevano. Revisiona continuamente la sua comprensione alla luce delle nuove evidenze e genera azioni autonome che si adattano alla minaccia nel momento in cui si palesa.

Ransomware

Rapidi e letali

Estorsione automatizzata

Alle 19.05 di un venerdì, un dipendente di una grande azienda di telecomunicazioni 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.

L'IA Darktrace ha reagito in pochi istanti. Solo nove secondi dopo l'inizio delle attività di crittografia SMB, Darktrace ha generato un allarme prioritario a indicare che l'anomalia richiedeva un'indagine immediata. Visto che il comportamento persisteva nei pochi secondi successivi, Darktrace ha revisionato il suo giudizio e ha attivato Antigena.

Dato che il team addetto alla sicurezza era andato a casa per il week-end, Darktrace Antigena ha risposto autonomamente interrompendo tutti i tentativi di scrivere i file crittografati nelle condivisioni di rete. Tale operazione ha neutralizzato all'istante la minaccia prima che potesse diffondersi in tutta l'infrastruttura diffusa delle telecomunicazioni, dando al team addetto alla sicurezza il tempo di rilevarla.

Poiché le specie automatizzate di ransomware continuano ad emergere sul dark web e nelle reti aziendali di tutto il mondo, le organizzazioni dovranno contrattaccare con l'IA per tenere il passo. Qui come altrove, la risposta dell'IA informatica di Darktrace è diventata una componente fondamentale nella lotta, contenendo attacchi ad azione rapida prima che abbiano il tempo di crittografare dati critici e arrestare

Spear Phishing

Un attacco mirato alle e-mail

Attacco alle e-mail

Un comune degli Stati Uniti è rimasto vittima di un attacco mirato, arrivato tramite e-mail. Anche se molti attacchi di phishing sono campagne "drive-by" indiscriminate, questa campagna portava la firma di un crimine informatico coordinato e sofisticato. Ogni e-mail era ben fatta e studiata per il destinatario previsto. L'actor della minaccia aveva utilizzato anche la rubrica degli indirizzi della città, poiché l'attacco era stato lanciato ai destinatari in ordine alfabetico, dalla A alla Z.

Anche se ciascuna e-mail sembrava innocua ed era creata su misura per il destinatario, i messaggi contenevano tutti un payload dannoso che nascondeva un pulsante che era camuffato in vari modi come link a Netflix, Amazon ed altri servizi fidati.

> Antigena ha individuato la minaccia alla lettera "A", gli strumenti esistenti solo alla "R"

Link nascosti

L'IA di Darktrace è riuscita ad analizzare questi link nascosti in associazione con i normali "pattern of life" dei destinatari previsti nella rete. Quando la prima e-mail è stata recapitata, Antigena ha riconosciuto immediatamente che né il destinatario né nessun altro del suo gruppo di colleghi o altri membri dello staff avevano mai visitato tale dominio. Antigena ha generato istantaneamente un allarme di alta sicurezza e ha suggerito autonomamente il blocco di ciascun link non appena entrava nella rete.

È interessante notare il fatto che Antigena sia stato utilizzato in "Modalità passiva", grazie all'evidenza semplice e concreta della capacità del sistema di sventare attacchi celati che altri strumenti non avrebbero rilevato: mentre Antigena ha individuato e cercato di neutralizzare la minaccia alla lettera "A", gli strumenti esistenti del team addetto alla sicurezza l'hanno individuata solo alla "R". In "Modalità attiva", Antigena avrebbe neutralizzato l'attacco prima che potesse raggiungere un singolo utente.

Attacco alla catena di distribuzione

Un impostore che ha sfruttato relazioni fidate

Account e-mail rubato

Alcuni dei più intraprendenti pirati informatici di oggi hanno imparato che il percorso più facile nell'ambiente dell'impresa spesso è attraverso la porta principale, purché riescano a ottenere la fiducia di un utente legittimo. Rubando i dettagli dell'account di un collega fidato, un business associate o fornitore nella catena di distribuzione, gli actor di minacce possono ingannare i destinatari e indurli a fare clic su un link dannoso o a trasferire milioni fuori dal business.

L'IA di Darktrace ha rilevato un simile attacco mirato ad uno studio di produzione cinematografica di Los Angeles, dopo che i dettagli di account di un contatto presso un fornitore fidato erano stati compromessi.

I dettagli dell'account possono essere usati per molti scopi nefasti, ma in questo caso, sembra che il criminale li abbia usati per leggere la cronologia della corrispondenza del contatto con un dipendente dello studio. Dopo aver revisionato i thread precedenti e imparato come comunicavano solitamente il contatto e il dipendente, ha inviato una risposta verosimile all'ultima e-mail del dipendente.

> L'e-mail era convincente, rispecchiava lo stile e il tono di scrittura del contatto

Crederci o no?

L'e-mail era convincente, rispecchiava lo stile e il tono di scrittura del contatto e aveva senso nel contesto della relazione e delle precedenti discussioni. Inoltre, includeva un link dannoso che sarebbe sembrato innocuo per qualsiasi dipendente sensibile che riceveva un link da un contatto familiare in un'azienda familiare. Questi tipi di attacchi stanno diventando sempre più comuni e molto difficili da rilevare.

L'IA informatica di Darktrace ha riconosciuto gli indicatori deboli che hanno rivelato che questo "contatto fidato" era un account rubato, controllato da un pirata. La risposta dell'IA ha preparato la rete mettendola a conoscenza che l'e-mail e il suo contenuto erano fuori dal "pattern of life" dell'ipotetico mittente. Il dipendente è stato avvisato e il payload dannoso è stato neutralizzato.

Fondamentalmente, la decisione di Antigena era informata del fatto che questo particolare link sarebbe stato raro sia per il mittente che per il destinatario, date le loro precedenti comunicazioni, e per i normali "pattern of life" del dipendente nella rete. Il team addetto alla sicurezza era sicuro del proprio livello di sicurezza, sapendo che l'IA di Darktrace non trattava il destinatario nella rete come un semplice indirizzo e-mail. Anzi, Antigena riconosce che l'intero ambito del "pattern of life" del dipendente spesso viene reso palese in vari angoli della rete e in un modo che può essere correlato e analizzato favorevolmente dall'IA informatica.

Contatti

Milano: +39 02 5821 5328

Roma: +39 06 3671 2329

Europa: +44 (0) 1223 394 100

Nord America: +1 (415) 1223 394 100

info@darktrace.com | darktrace.com/it

@darktrace