Panoramica di settore: retail

Mentre i retailer fanno sempre più affidamento sui sistemi digitali per massimizzare la facilità d'uso e le personalizzazioni per i propri clienti, i pirati informatici si adeguano per sfruttare questi cambiamenti nel panorama informatico. Le aziende in tutto il mondo stanno adottando la self-learning AI per individuare i primi segnali di comportamenti anomali che indicano un attacco informatico in corso, rilevando e bloccando minacce mai viste in precedenza che sono in grado di eludere gli strumenti di sicurezza tradizionali.

In sintesi

- ✔ Protegge centinaia di clienti retail in tutto il mondo
- ✔ La tecnologia di self-learning AI protegge i progetti di trasformazione
- ✔ L'Autonomous Response blocca chirurgicamente le minacce informatiche prima che causino problemi
- ✔ Cyber AI Analyst automatizza le indagini relative alla sicurezza

Come i pirati informatici sfruttano i cambiamenti nel settore retail

I pirati informatici utilizzano schemi sofisticati per colpire i retailer e l'enorme quantità di informazioni personali e finanziarie dei loro clienti. Di solito questo panorama delle minacce si intensifica in determinati momenti dell'anno: Darktrace ha rilevato un aumento del 128% di attacchi trojan nel periodo compreso tra novembre e dicembre 2020 rispetto ai mesi precedenti. Anche lontano dai periodi festivi il volume di attacchi ai danni del settore retail sono raddoppiati nel corso dei primi mesi del 2021, in parte a causa dei cambiamenti globali legati allo smart working.

Poiché il commercio continua sempre più a svilupparsi online, gli stack di cyber security sono diventati fondamentali per poter sopravvivere. Se il sito web di un'azienda è offline a causa di un attacco, le perdite possono essere disastrose se non addirittura fatali per l'operatività aziendale. Negli anni scorsi, le minacce all'e-commerce, incluso lo skimming online, sono progressivamente aumentate.

Un altro motivo di preoccupazione è l'aumento dell'utilizzo da parte del settore di dispositivi collegati a Internet. Il tipico ambiente retail ha un rapporto dispositivi-persone di 5:1, cioè ogni 100 dipendenti ci sono 500 dispositivi che devono essere protetti. Queste reti distribuite complicano la cyber security e aumentano la superficie di attacco disponibile per i pirati informatici.

I pirati informatici continuano a prendere di mira i sistemi Point of Sale (POS) collegati e online perché molti retailer non utilizzano ancora una crittografia end-to-end. Ad esempio, i malware memory-scraper ("raschia memoria"), in grado di eseguire la scansione e poi esfiltrare i dati delle carte di credito e dei bancomat dai sistemi POS, rimangono il pericolo principale.

> "Quando si parla di sicurezza efficace l'AI è sicuramente un elemento fondamentale. La combinazione di fattore umano e AI è ciò che serve oggi per la sicurezza."
>
> Leon Shepherd, CIO, Ted Baker

> "Il settore retail è continuamente colpito da attacchi informatici, ecco perché abbiamo scelto l'innovativa tecnolgia di Darktrace per rilevare potenziali attacchi prima che possano causare problemi."
>
> Dane Sandersen, Global Security Director, Trek

Un approccio basato sull'Immune System per l'eCommerce

I principali retailer di tutto il mondo hanno scelto Darktrace per proteggere i loro ecosistemi digitali in continua evoluzione contro attacchi sempre più sofisticati. Sfruttando la self-learning AI, Darktrace identifica e blocca minacce nuove e imprevedibili all'interno di tutta l'organizzazione, da ransomware ad attacchi ai sistemi POS, da campagne di spear phishing a compromissioni di siti web.

Improntata sul funzionamento del sistema immunitario dell'uomo, la Cyber AI di Darktrace apprende continuamente ciò che è "normale" per ogni utente e dispositivo all'interno di un'organizzazione e per tutti i collegamenti che intercorrono tra di essi. Ciò consente all'AI di rilevare gli impercettibili segnali di una minaccia non appena emerge, indipendentemente da quanto sia sofisticata, inedita o imprevedibile. Antigena, la tecnologia di Autonomous Response di Darktrace, neutralizza poi chirurgicamente la minaccia alla velocità delle macchine, garantendo così il normale svolgimento dell'operatività aziendale.

Per aiutare e aumentare le capacità dei team della sicurezza, questa funzionalità viene abbinata a Cyber AI Analyst, che indaga, analizza e segnala autonomamente gli incidenti di sicurezza. I report generati da Cyber AI Analyst consentono ai team di agire non appena la minaccia viene rilevata, riducendo così del 92% il tempo di analisi.

Darktrace agisce all'interno dell'intero ecosistema digitale, da applicazioni Cloud e SaaS ad ambienti di posta elettronica e IoT, aiutando i team della sicurezza a proteggere i dati sensibili relativi ai clienti e le registrazioni finanziarie ovunque si trovino.

Rilevamento della minaccia: bloccare lo sviluppo del ransomware Sodinokibi

Nell'agosto 2020, Darktrace ha scoperto la presenza del ransomware Sodinokibi presso un cliente retail. Sodinokibi è un esempio di Ransomware-as-a-Service (RaaS, "ransomware come servizio"), un fenomeno preoccupante che consente ai pirati informatici di basso livello di lanciare attacchi evoluti.

L'attacco era iniziato quando un dispositivo aveva avviato attività amministrative anomale, prima di scrivere un file eseguibile insolito e condividerlo con altre risorse interne. Il dispositivo poi era passato a crittografare numerosi file in rete e a scrivere note di riscatto. Subito dopo il dispositivo aveva eseguito numerose scansioni della rete, alla ricerca di ulteriori canali aperti da sfruttare. Tutto ciò accadeva in pochi minuti, dimostrando con quale velocità un ransomware sia in grado di muoversi all'interno delle reti aziendali.

La self-learning AI di Darktrace aveva avvisato il team della sicurezza a ogni fase, consentendo di rispondere all'attacco in corso. Se Antigena fosse stato attivato, l'attacco sarebbe stato bloccato fin dall'inizio, interrompendo in pochi secondi qualsiasi attività pericolosa.

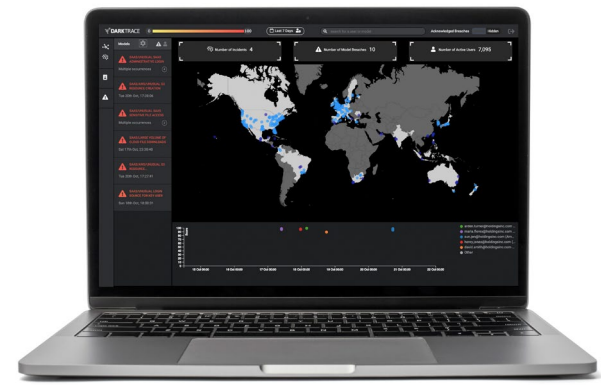
> "Avere la tecnologia di Darktrace basata sull'AI che apprende e migliora costantemente è molto meglio che utilizzare strumenti di auditing."
>
> James Bywater, IT Infrastructure Manager, PizzaHut

Le minacce in numeri

1° settore più colpito dai ransomware nel 2020.

4,2 miliardi pagati dalle organizzazioni a causa di ransomware a doppia estorsione nel 2020.

70% di shopping effettuato online nel dicembre 2020, rispetto al 55% del 2019.



La console SaaS di Darktrace evidenzia attività utente anomale per rilevare minacce basate su Cloud e SaaS