Acronis Utilizzo del Machine Learning per proteggere i dati

Introdotto nel gennaio 2017, Acronis Active Protection è una tecnologia avanzata che sfrutta l'analisi avanzata per monitorare i sistemi alla ricerca di comportamenti di tipo ransomware e per arrestarli rapidamente. Nonostante i risultati positivi di test indipendenti e i riconoscimenti dei media, Acronis ha voluto rendere la soluzione ancora più robusta. Abbiamo raggiunto lo scopo con successo sfruttando il machine learning e le tecnologie di intelligenza artificiale.

L'AIUTO DEL MACHINE LEARNING

Il machine learning è spesso un termine associato a grandi dati: l'analisi di enormi volumi di dati per produrre risultati attuabili. Poiché il machine learning è basato sulla quantità di dati e sugli algoritmi scelti, più grande è il campione di dati, migliori saranno i risultati.

In che modo Acronis utilizza questa tecnologia? Il primo passo consiste nell'eseguire un'analisi delle tracce stack che riporta le subroutine del programma. Questa tecnica viene comunemente utilizzata per alcuni tipi di debug, aiutando gli ingegneri del software a capire dove risiede un problema o come varie subroutine lavorano insieme durante l'esecuzione.

Acronis applica questo approccio a un attacco ransomware, utilizzando l'apprendimento automatico per rilevare le iniezioni di codice dannose.

COME FUNZIONA IL MACHINE LEARNING

Acronis ha analizzato enormi volumi di dati non infetti utilizzando sistemi Windows che eseguono decine di processi legittimi. Da questi processi abbiamo, quindi, ottenuto milioni di tracce stack legittime e abbiamo costruito diversi modelli di comportamento "buono" utilizzando l'apprendimento delle strutture decisionali. Abbiamo anche raccolto tracce stack dannose da varie fonti per fornire controesempi.

In base a questi milioni di campioni di apprendimento, vengono identificati modelli di comportamento.

Con l'apprendimento delle strutture decisionali, possiamo passare dall'osservazione di un elemento, per trarre conclusioni sul suo valore obiettivo, alla creazione di un modello che predica in modo accurato il valore di un nuovo elemento basato su fattori identificabili. I modelli consentono ad Acronis di integrare risposte adeguate ai valori obiettivi. Piuttosto che rallentare la macchina client raccogliendo e inviando dati da analizzare, i modelli integrati offrono lo stesso livello di protezione con maggiore efficienza.

QUANDO SI ATTIVA IL MACHINE LEARNING?

Come affermato in precedenza, Acronis Active Protection si basa sull'euristica comportamentale. Nella versione 2.0 abbiamo aggiunto diverse nuove euristiche che cercano processi legittimi. Se Acronis Active Protection rileva un comportamento anomalo in un processo legittimo, preleva una traccia dello stack e la invia al modulo del machine learning di Acronis. Qui il comportamento viene confrontato con i modelli esistenti di tracce stack infette e non infette per determinare se si tratta di una minaccia o meno.

Se si stabilisce che il comportamento presenta una natura dannosa, l'utente riceve un avviso che suggerisce di bloccare il processo.

NUOVO LIVELLO DI PROTEZIONE ANTI-RANSOMWARE

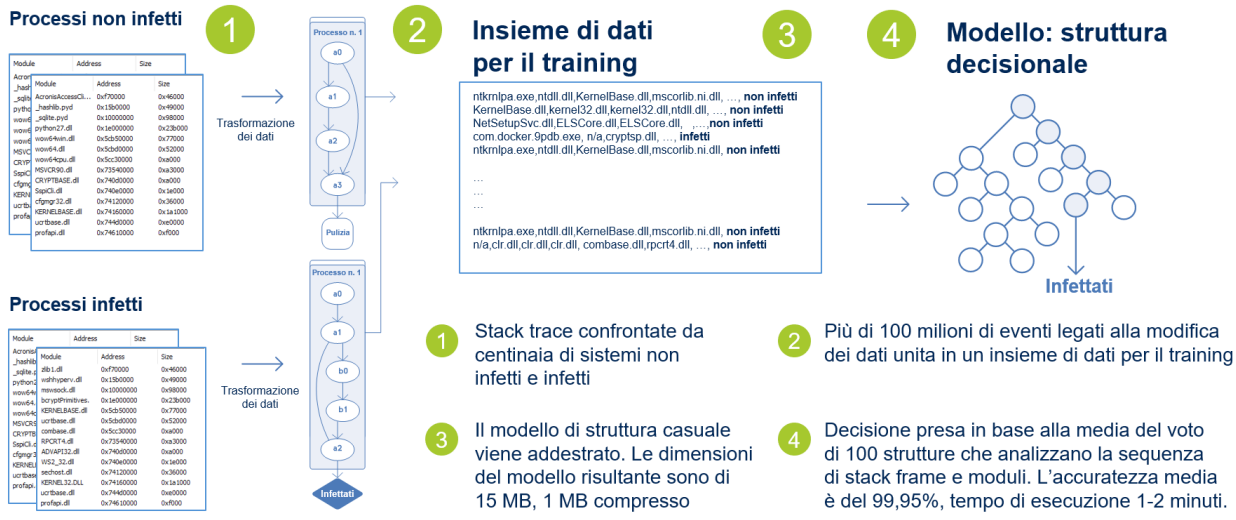
Con il machine learning all'avanguardia, tutte queste tecnologie portano Acronis Active Protection a un livello completamente nuovo, specialmente quando si tratta di combattere le minacce zero-day. Esso crea un modello per processi legittimi, quindi anche se gli aggressori trovano una nuova vulnerabilità o un modo per infiltrarsi nel sistema, il machine learning rileverà i processi del ransomware e li bloccherà.

L'infrastruttura del machine learning di Acronis è costruita in modo tale che i nuovi dati resi anonimi del programma vengano caricati regolarmente per l'analisi. Questa infrastruttura è in grado di gestire milioni di richieste simultaneamente e, grazie al costante flusso di informazioni, i nuovi modelli comportamentali sono pronti in modo estremamente più rapido. Nel frattempo, gli aggiornamenti costanti dell'euristica dei prodotti aumentano ulteriormente la sicurezza. Nessuna parte di questo lavoro discreto e puntuale è visibile agli utenti: ad essi basta semplicemente attivare Acronis Active Protection e dimenticarsene.

LE PROSSIME NOVITÀ

Acronis continua a espandere l'uso di questa tecnologia utilizzando il machine learning per l'analisi del codice statico. Questa analisi verrà eseguita nella fase di pre-esecuzione; pertanto, quando si scarica un file o si copia un file su un disco rigido, il relativo codice verrà immediatamente controllato per rilevare eventuali anomalie. Se emerge qualcosa di sospetto, il processo può essere bloccato prima che venga lanciato da un utente o da uno script automatico.

In effetti, i modelli di machine learning possono essere utilizzati per analizzare gli script e Acronis sta già lavorando in questa direzione. A prova di ciò, i test di NioGuard Security Lab hanno dimostrato che mentre la maggior parte delle soluzioni antivirus non sono in grado di rilevare un attacco basato su script, Acronis Active Protection funziona perfettamente. Nonostante questo successo, continueremo a migliorare ulteriormente le nostre tecnologie anti-ransomware.



Per maggiori informazioni, visitate il sito **www.acronis.com**