Acronis

WHITE PAPER

Utilizzare l'AI per individuare documenti e script pericolosi

Protezione avanzata a più livelli basata su machine intelligence

L'aumento degli attacchi digitali è costante e sempre più criminali informatici utilizzano come vettore principale le tecniche di social engineering, diffuse tramite e-mail e altri canali di comunicazione. Spesso le e-mail ingannevoli contengono allegati pericolosi che, una volta aperti, innescano l'esecuzione di un malware che agisce in modo doloso sfruttando le vulnerabilità dei sistemi. I documenti pericolosi possono anche essere scaricati cliccando sui link ricevuti tramite altri canali di comunicazione.

Secondo gli esperti Acronis, circa un terzo di tutti gli attacchi sferrati nel primo semestre del 2022 sono stati innescati da documenti di Microsoft Office o da file PDF trasformati in strumenti per infiltrarsi nei sistemi. Un quadro simile è riferito anche da altri operatori del settore. Il malware si cela sempre dentro un file, sebbene la sequenza di esecuzione possa variare. In genere, il primo passo è l'exploit della vulnerabilità, a cui segue l'elevazione dei privilegi e quindi il download e l'esecuzione del malware. Da anni ormai, i file di Microsoft Office e i PDF di Adobe vengono utilizzati negli attacchi informatici, perché sono in grado di incorporare macro, shellcode, JavaScript e perfino interi file. Negli ultimi anni il problema si è aggravato: ora gli hacker utilizzano le tecniche di ottimizzazione per i motori di ricerca (SEO) per far sì che i documenti infetti, in primo luogo i PDF, vengano visualizzati ai primi posti nei risultati dei motori di ricerca.

Un problema simile è quello legato agli script dannosi eseguiti da strumenti legittimi, come PowerShell. Anche il numero di attacchi sferrati tramite tali script dannosi cresce costantemente, ma negli ultimi due anni la diffusione è raddoppiata, affermano gli esperti di Acronis. L'obiettivo degli script malevoli è lo stesso: infiltrarsi nel sistema, elevare i privilegi, scaricare e quindi eseguire il payload.

Le aziende che si occupano di Cyber Security non fanno differenza tra le due problematiche appena evidenziate, perché entrambe comportano il dover distinguere documenti e script tra "buoni" o "cattivi". Fortunatamente, oggi il problema può essere risolto più efficacemente con l'utilizzo del machine learning (ML) e dell'intelligenza artificiale (AI), una combinazione che Acronis definisce machine intelligence (MI).

Utilizzare la machine intelligence per rilevare le minacce

Acronis si avvale del machine learning già dal 2017, anno in cui l'azienda ha introdotto la tecnologia Active Protection per individuare il ransomware. Poco dopo, fu creato un motore di rilevamento statico completamente basato su intelligenza artificiale, che è ancora utilizzato nel prodotto di punta di Acronis, Acronis Cyber Protect.

Il motore è costantemente aggiornato e con ogni nuovo modello di machine learning introdotto ottiene risultati migliori in termini di prestazioni e tasso di rilevamento. Nelle prime fasi, ad esempio, era utilizzato per analizzare le tracce stack dei processi eseguiti, e in seguito per analizzare interi file e librerie e identificare quelli pericolosi. Ora è in grado di esaminare stringhe estratte da file eseguibili e di elaborare immagini. La funzionalità aggiuntiva che estrae le stringhe di testo ed esamina la frequenza con cui ricorrono alcune centinaia di parole selezionate ha permesso di migliorare di oltre il 3% il tasso di rilevamento.

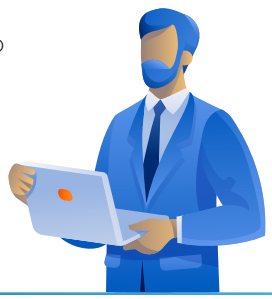
Come si può immaginare, un approccio analogo può essere adottato per individuare documenti e script pericolosi. Iniziamo dai documenti di Microsoft Office. Benché Microsoft abbia di recente presentato e introdotto l'approccio che prevede la disattivazione predefinita delle macro nei documenti trasmessi tramite Internet, questo non basta, purtroppo, a risolvere tutti i problemi. Windows aggiunge ai file che provengono da una fonte non attendibile, come Internet o un'area soggetta a restrizioni, ad esempio i download da browser o gli allegati alle e-mail, l'attributo chiamato Mark of the Web (MOTW). Tuttavia, l'attributo è applicabile soltanto ai file salvati su un file system NTFS e non a quelli salvati su dispositivi con formattazione FAT32. E cosa succede se il file proviene da un indirizzo e-mail legittimo? Nei contesti fortemente dipendenti dalle macro, ad esempio i reparti di contabilità, l'approccio potrebbe non essere adatto. Può comunque rendere più sicuro un ambiente regolamentato da policy, e in alcuni casi specifici di tentativi di phishing, come quelli delle campagne Emotet, consente una prevenzione efficace. Come già detto, tuttavia, non è sufficiente e può causare ulteriori complicazioni in molti settori. Per questo gli specialisti Acronis che si occupano di intelligenza artificiale hanno migliorato il motore di rilevamento, affinché individui i documenti pericolosi sfruttando le potenzialità del machine learning.

Possono essere identificati come pericolosi script di macro che eseguono una o più delle attività seguenti:

- Creazione di processi
- Esecuzione di script in PowerShell, VBA, ecc.
- Download di file da server remoti
- Incorporazione in altri file di Office o in file modelli di Office

L'effettivo rilevamento non è così semplice, poiché occorre tenere in considerazione molti parametri. Per valutare correttamente un file, il modello di machine learning di Acronis controlla, ad esempio, i seguenti attributi dei file DOCX:

- Funzionalità varie per testi e funzioni VBA
- Giuste proporzioni tra commenti, codice, ecc.
- Analisi dell'entropia della macro in sé, del codice e dei commenti
- Presenza di eventuali offuscamenti e tipo di elemento offuscato
- Parametri relativi agli indicatori di compromissione noti (IoC) come URL, file eseguibili, ecc.



Non è certo un elenco esaustivo, ma aiuta a far capire la quantità di elementi oggetto di analisi in un dataset di grandi dimensioni, che viene continuamente rivisto e aggiornato. In sostanza, con un modello compresso che ha una dimensione inferiore a 1 MB, otteniamo un eccellente tasso di rilevamento. Senza AI e ML, ottenere risultati di questo tipo è praticamente impossibile. Quanto illustrato è soltanto una parte della solida protezione a più livelli che si innesca solo se la minaccia non è stata rilevata da altre tecnologie, come i motori di scansione e gli ambienti sandbox per la sicurezza e-mail, o il filtraggio degli URL.

Un approccio molto simile è stato recentemente introdotto dagli esperti Acronis per rilevare script AutoIT malevoli, spesso utilizzati negli ambienti dei Service Provider. Un piccolo modello di circa 0,6 MB è già in grado di fornire un tasso di rilevamento del 92%, e lo stesso vale per il formato DOCX, il cui modello viene migliorato costantemente.

Estirpare la minaccia dei PDF ingannevoli

Oltre ai documenti di Microsoft Office Word, anche il formato Adobe Portable Document, o PDF, è uno strumento molto diffuso con il quale i criminali informatici compromettono sistemi o infiltrano malware nei computer degli utenti. Basato sul linguaggio PostScript, il PDF costituisce un formato molto versatile che può contenere svariate informazioni, tra cui testi, link, elementi multimediali, immagini, allegati, metadati, ecc. Può prevedere inoltre alcune funzioni di "azione" che permettono l'apertura di collegamenti web o file, l'esecuzione di codice JavaScript e diverse altre operazioni, molte delle quali possono avere un intento doloso.

I documenti PDF possono essere visualizzati da browser e con numerosi software di lettura, che a loro volta presentano o potrebbero presentare vulnerabilità sfruttabili dagli autori delle minacce per l'esecuzione di codice arbitrario, overflow del buffer, danneggiamento della memoria, operazioni di lettura fuori limite e molte altre. Ad oggi sono state individuate centinaia di CVE nei lettori di PDF, con oltre 300 vulnerabilità note nel solo Adobe Acrobat Reader. Praticamente ogni giorno i ricercatori nell'ambito della sicurezza (ma anche gli autori delle minacce) individuano nuovi potenziali exploit legati ai PDF.

Di seguito è riportato un esempio che mostra la vulnerabilità CVE-2021-28550 così come è stata osservata in circolazione. Le versioni di Acrobat Reader DC 2021.001.20150 (e precedenti), 2020.001.30020 (e precedenti) e 2017.011.30194 (e precedenti) sono interessate da una vulnerabilità "use-after-free". Un attaccante non autenticato potrebbe sfruttare questa vulnerabilità per avviare l'esecuzione di codice arbitrario nell'ambiente dell'utente corrente. Per questo exploit è necessaria l'interazione dell'utente, ovvero la vittima deve aprire il file malevolo.

Esempio di phishing con un link malevolo inserito in un file PDF

Come per i tipi di file descritti in precedenza, il modello Acronis di machine learning per il rilevamento dei PDF pericolosi controlla numerosi parametri per giungere a un esito corretto:

- Entropia
- Conteggio totale dei caratteri
- Conteggio delle parole chiave speciali
- Numero di righe, righe con assegnazioni speciali
- Ecc.

Anche in questo caso il tasso di rilevamento è identico e altamente efficace.

Un valido aiuto: la formazione sulla Cyber Security degli operatori

È fondamentale integrare questo tipo di modello di rilevamento in una valida soluzione di Cyber Protection. Il profilo di sicurezza dei singoli individui e dell'azienda nel suo complesso migliora nettamente se gli utenti sono consapevoli delle minacce e del mondo in cui si presentano e se sanno come reagire adeguatamente, poiché nella maggior parte dei casi è necessario l'input dell'utente per attivare un documento o uno script dannoso. Se questo input viene a mancare, non si avrà alcuna minaccia.

Essere consapevoli dei rischi di sicurezza significa rispettare alcune regole ben note:

- Controlla sempre la provenienza di e-mail e link. Conosci il mittente? Aspettavi il file? Accertati di controllare l'indirizzo e-mail reale da cui arriva il messaggio, non solo il nome o l'alias del mittente.
- Nel caso in cui avessi già cliccato sul file e si sia aperto un messaggio che indica una qualche incompatibilità o chiede di attivare qualcosa, visualizzare un link o un captcha fasullo o elementi simili, il file deve essere immediatamente chiuso ed eliminato, ed è necessario avvisare il team della sicurezza.
- È un brutto segnale anche se hai cliccato sul file ma non si apre nulla. Se hai aperto il file ma non contiene ciò che ti aspettavi, potresti essere vittima di un attacco e devi informare il team di sicurezza immediatamente.

La regola più efficace è non aprire allegati e non cliccare sui collegamenti diretti. Controlla sempre due volte, e se hai ancora qualche dubbio, consulta il team di sicurezza. Stai sempre all'erta e resta al sicuro.

Acronis

Per saperne di più, visita
www.acronis.com