SOPHOS
Security made simple.

Intercept X Deep Learning

Intercept X łączy funkcję głębokiego uczenia z najlepszą w swojej klasie technologią zapobiegającą wykorzystywaniu luk, technologią CryptoGuard chroniącą przed programami ransomware, funkcją analizowania źródeł problemów i innymi funkcjami, tworząc najbardziej wszechstronne rozwiązanie ochrony urządzeń końcowych dostępne w branży. To wyjątkowe połączenie funkcji sprawia, że pakiet Intercept X zatrzymuje największą liczbę zagrożeń urządzeń końcowych.

Najważniejsze informacje

- Najlepszy mechanizm wykrywania złośliwego oprogramowania
- Zapobiega zarówno znanemu, jak i dotąd niespotykanemu złośliwemu oprogramowaniu
- Blokuje złośliwe oprogramowanie zanim zostanie uruchomione
- Nie bazuje na sygnaturach
- Chroni system nawet wtedy, gdy host jest odłączony od sieci
- Wykrywa złośliwe oprogramowanie w około 20 milisekund
- Przeszedł proces uczenia z wykorzystaniem setek milionów próbek
- Od sierpnia 2016 skuteczność potwierdzona przez witrynę VirusTotal
- Klasyfikuje pliki jako złośliwe, aplikacje potencjalnie niechciane (PUA) lub pliki nieszkodliwe
- Działa w konfiguracji standardowej bez konieczności dodatkowego uczenia
- Zajmuje wyjątkowo mało miejsca (poniżej 20 MB)
- Skupia się na przenośnych plikach wykonywalnych systemu Windows

Większość dzisiejszych rozwiązań zabezpieczających działa w sposób interwencyjny i stanowczo zbyt wolny. Ponieważ liczba i złożoność ataków na urządzenia końcowe stale rośnie, dotychczasowe rozwiązania z trudem dotrzymują im tempa. Laboratorium SophosLabs analizuje na przykład codziennie ponad 400 000 nowych próbek złośliwego oprogramowania. Okazuje się, że wyzwaniu sprostać jeszcze trudniej, ponieważ według SophosLabs 75% złośliwego oprogramowania charakteryzuje wyłącznie pojedyncze organizacje.

Deep Learning, zaawansowana forma uczenia maszynowego, pomaga zmieniać sposób podejścia do ochrony urządzeń końcowych, a rozwiązanie Intercept X jest liderem tej zmiany. Dzięki zastosowaniu mechanizmu deep learning Intercept X zmienia podejście do ochrony urządzeń końcowych z interwencyjnego na predykcyjne, dzięki czemu jest w stanie skutecznie chronić przed nieznanymi zagrożeniami.

Deep Learning w porównaniu do innych typów uczenia maszynowego

„Intercept X wykorzystuje głęboką sieć neuronową, która działa podobnie, jak ludzki mózg... W efekcie zyskujemy wysoki wskaźnik dokładności wykrywania zarówno w przypadku istniejącego złośliwego oprogramowania, jak i oprogramowania typu „zero-day", jak również niższy wskaźnik błędów fałszywie pozytywnych".

Raport ESG Lab, grudzień 2017 r.

Mimo że wiele produktów rzekomo wykorzystuje uczenie maszynowe, nie wszystkie metody takiego uczenia są sobie równoważne. W Sophos do wykrywania złośliwego oprogramowania wykorzystujemy głębokie uczenie. Głębokie uczenie, nazywane również „głębokimi sieciami neuronowymi" albo „sieciami neuronowymi", zostało zainspirowane sposobem działania ludzkiego mózgu. Taki sam typ uczenia maszynowego jest często używany do rozpoznawania twarzy, przetwarzania języka naturalnego, w pojazdach autonomicznych oraz w innych zaawansowanych dziedzinach nauki i badań informatycznych.

Deep Learning stale znacznie przewyższa inne modele uczenia maszynowego, w tym metody random forest, metody grupowania centroidów (k-średnich) czy sieci bayesowskie, jednak do zbudowania efektywnego modelu wymaga ogromnej ilości danych oraz dużej mocy obliczeniowej. W Sophos udało się to zrobić w prosty sposób dzięki kolekcji złośliwego oprogramowania i wysiłków SophosLabs włożonych w jego analizę w ciągu ostatnich

30 lat, jak również dzięki danym telemetrycznym odbieranym codziennie z ponad 100 milionów urządzeń końcowych.

W porównaniu do innych modeli uczenia maszynowego wykorzystywanych powszechnie do ochrony urządzeń końcowych, oferuje wiele nieodłącznych korzyści:

Bardziej inteligentne rozwiązanie: Modele głębokiego uczenia przetwarzają dane w wielu warstwach analizy, podobnie jak neurony w ludzkim mózgu. Każda warstwa sprawia, że model staje się znacznie bardziej wydajny. Analizowane są złożone zależności między różnymi funkcjami wejściowymi. Pozwala to na automatyczne odkrywanie najlepszych kombinacji i manipulowanie danymi wejściowymi, co dla człowieka byłoby po prostu niemożliwe. Oznacza to, że model Sophos wykrywania złośliwego oprogramowania w oparciu o głębokie uczenie jest w stanie wykrywać złośliwe oprogramowanie, które w przypadku innych mechanizmów uczenia maszynowego pozostałoby niezauważone.

Lepsza możliwość rozbudowy: Deep Learning zgrabnie skaluje się do setek milionów próbek do wyuczenia. To bardzo ważne, jeśli uwzględnimy fakt, że w SophosLabs analizujemy 2,8 miliona nowych próbek złośliwego oprogramowanie tygodniowo. Ponieważ nasz model może stale przetwarzać niesamowite ilości danych do wyuczenia, potrafi „zapamiętywać" cały obserwowalny krajobraz zagrożeń w ramach procesu uczenia.Ponieważ głębokie uczenie może przetwarzać znacznie więcej danych niż inne modele, metoda ta jest w stanie skutecznie przewidywać dzisiejsze zagrożenia i jednocześnie stale być na bieżąco.

Mniejszy rozmiar: Tradycyjne metody uczenia maszynowego powodują powstawanie modeli ogromnych rozmiarów, które czasami mogą zajmować na dysku wiele gigabajtów. Z drugiej strony głębokie uczenie zastosowane przez firmę Sophos generuje bardzo skompresowane modele.Model głębokiego uczenia Sophos jest niesamowicie mały. Zajmuje na urządzeniu końcowym mniej niż 20 MB i ma niemal zerowy wpływ na jego wydajność.

Możliwości głębokiego uczenia Sophos

Sophos oferuje specjalistyczną wiedzą z zakresu głębokiego uczenia z wykorzystaniem najbardziej skutecznego mechanizmu wykrywania złośliwego oprogramowania na rynku:

Doświadczenie: W przeciwieństwie do konkurencji jesteśmy od wielu lat ekspertami od uczenia maszynowego w dziedzinie cyberbezpieczeństwa. Nasze modele wykrywania złośliwego oprogramowania za pomocą głębokiego uczenia działają od lat w środowiskach produkcyjnych. Model wykrywania złośliwego oprogramowania Sophos został opracowany przez nasz zespół analityków danych z wykorzystaniem technologii stosowanej w DARPA.

W 2010 roku agencja DARPA (Advanced Research Projects Agency) Departamentu Obrony Stanów Zjednoczonych stworzyła program Cyber Genome w celu odkrycia „DNA" złośliwego oprogramowania oraz innych zagrożeń cyfrowych.Były to początki algorytmu, który obecnie jest wbudowany w rozwiązanie Intercept X.

Sprawdzone działanie: Nasze modele są otwarte i przejrzyste. Oprócz prezentowania szczegółów naszej metodologii na konferencjach branżowych (np. Black Hat), pozwalamy także testować nasz model niezależnym firmom zewnętrznym. Skuteczność modelu jest potwierdzana od sierpnia 2016 przez witrynę VirusTotal, otrzymuje on również wysokie wyniki punktowe od niezależnych firm testujących, takich jak NSS Labs.W każdym przypadku okazał się wyjątkowo skuteczny, wykazując niewielką liczbę fałszywych zagrożeń.

„To jeden z najlepszych wyników, jaki kiedykolwiek uzyskaliśmy w naszych testach".

Maik Morgenstern, CTO, AV-TEST

Wydajność: Technologia modelu głębokiego uczenia Sophos jest niezwykle szybka. Krócej niż w ciągu 20 milisekund model jest w stanie wyodrębnić z pliku miliony parametrów, przeprowadzić głęboką analizę oraz określić, czy plik jest nieszkodliwy czy złośliwy.Cały proces jest realizowany przed wykonaniem pliku.

SophosLabs: Jeden z najważniejszych aspektów każdego modelu to dane używane do uczenia. Nasz zespół analityków danych stanowi część grupy SophosLabs, co zapewnia mu dostęp do setek milionów próbek. Pozwala to wprowadzać do naszych modeli najlepsze możliwe predykcje. Zintegrowanie tych dwóch grup prowadzi również do lepszego klasyfikowania danych (a więc lepszego modelowania).Dwukierunkowa wymiana wiedzy na temat zagrożeń oraz informacji zwrotnych napływających z prawdziwych urządzeń końcowych, zachodząca między zespołem analityków danych a zespołem badającym zagrożenia, pozwala stale zwiększać skuteczność naszych modeli.

„Zapora Intercept X zatrzymała każdy skomplikowany, zaawansowany atak, który na nią przypuściliśmy".

Raport ESG Lab, grudzień 2017 r.

Wypróbuj teraz za darmo

Zarejestruj się i odbierz bezpłatną, 30-dniową wersję testową pod adresem sophos.com/interceptx

Dział sprzedaży w Polsce:Sophos Ltd. (Poland)
ul. Rzymowskiego 53, 02-697 Warszawa
Email: salesee@sophos.com

18-01-02 DS PL (2897-DD)

SOPHOS