SOPHOS
Security made simple.

Intercept X Deep Learning (mély tanulás)

Az Intercept X a mély tanulást a kategória legjobb biztonságirés-ellenes technológiájával, a CryptoGuard zsarolóprogram-ellenes technológiával, az alapvető okok elemzésével, valamint egyéb funkciókkal kombinálja az iparág legátfogóbb végpontvédelme érdekében. A funkcióknak ez az egyedi kombinációja lehetővé teszi, hogy az Intercept X a végponti fenyegetések legszélesebb körét állítsa meg.

Főbb jellemzők

- A legjobban teljesítő kártevőészlelő motor
- Mind az ismert, mind a még soha nem látott kártevőket megakadályozza
- A végrehajtás előtt megakadályozza a kártevőket
- Nem aláírások alapján működik
- Akkor is védelmet nyújt, amikor a gazdagép nem érhető el
- A kártevőket kb. 20 milliszekundum alatt észleli
- A betanítása több száz millió minta alapján történt
- 2016 augusztusa óta bizonyít a VirusTotalon
- A fájlokat rosszindulatúként, vélhetően nemkívánatos alkalmazásként (potentially unwanted apps, PUA) vagy jóindulatúként osztályozza
- Gyári formájában működik, nincs szükség további képzésre
- Rendkívül kis helyigény (kevesebb mint 20 MB)
- A Windows hordozható végrehajtható fájljaira koncentrál

A mai biztonsági megoldások nagy része csak reagálni képes, és túl lassú. A végponti támadások számának és bonyolultságának növekedésével a régimódi megközelítések nehezen tartják a lépést. A SophosLabs például minden nap több mint 400 000 új rosszindulatú-mintát elemez. Tovább nehezíti ennek a kihívásnak való megfelelést, hogy a SophosLabs arra jutott, hogy a rosszindulatú programok 75%-a egyetlen szervezetben található csak meg.

A mély tanulás a gépi tanulás egy fejlett formája, amely a végponti biztonság újfajta megközelítéseit teszi lehetővé, és ebben a változásban az Intercept X jár élen. A mély tanulás integrálásának köszönhetően az Intercept X a végponti biztonságot reaktív megközelítésből prediktív megközelítéssé változtatja, hogy védelmet nyújtson az ismeretlen fenyegetések ellen.

A mély tanulás összehasonlítása más gépi tanulási formákkal

„Az Intercept X mély tanulást megvalósító neurális hálózatot használ, ami úgy működik, mint az emberi agy... Ennek eredményeképpen nagyon pontosan felismeri mind a meglévő, mind a nulladik napi kártevőket, ugyanakkor alacsonyabb a hamis pozitívak aránya."

ESG laboratóriumi jelentés, 2017. december

Miközben sok termék azt állítja, hogy gépi tanulást alkalmaz, nem minden gépi tanulás ugyanolyan. A Sophosnál mély tanulást használunk a kártevők észlelésére. A mély tanulást „mély tanulást megvalósító neurális hálózatok" vagy „neurális hálózatok" néven is ismerik, alapja pedig az emberi agy működése. Ugyanaz a típusú gépi tanulás, amelyet gyakran használnak arcfelismeréshez, természetes nyelvek feldolgozásához, önvezető autókhoz, valamint a számítástechnika és kutatás egyéb vezető területein.

A mély tanulás következetesen jobban teljesít az egyéb olyan gépi tanulási modelleknél, mint a véletlen erdő (random forest), k-means klaszterezés vagy a Bayes-féle hálózatok, ugyanakkor egy hatékony modell kiépítéséhez rengeteg adatot és számítástechnikai teljesítményt igényel. A Sophosnál ezt a SophosLabs elmúlt 30 évben végzett kártevőgyűjtési és elemzési munkája, valamint a minden egyes nap több mint 100 millió végponttól érkező telemetria könnyítette meg.

A végponti biztonságban gyakran alkalmazott gépi tanulás más típusaihoz képest a mély tanulás számos velejáró előnyt kínál:

Okosabb: A mély tanulási modellek az emberi agy neuronjaihoz hasonlóan az adatokat több elemzési rétegen keresztül dolgozzák fel, és a modellt mindegyik réteg lényegesen hatásosabbá teszi. A módszer a különböző bemeneti tulajdonságok közötti bonyolult kapcsolatokat elemzi. Ez lehetővé teszi az olyan bemenetek legjobb kombinációjának és manipulálásának automatikus felfedését, amelyeket az emberek más módon nem tudnának megállapítani. Ez azt jelenti, hogy a Sophos mély tanulásos kártevő-észlelési modellje olyan kártevőket is képes észlelni, amelyeket más gépi tanulási motorok nem vennének észre.

Méretezhetőbb: A mély tanulás elegánsan méretezhető több millió tanulási mintához. Ez fontos, ha figyelembe vesszük, hogy a SophosLabs minden héten 2,8 millió új kártevőmintát elemez. Mivel hatalmas mennyiségű tanulási adatot tud folyamatosan betölteni, a modellünk a tanulási folyamat során képes a teljes belátható fenyegetéshalmaz „memorizálására". Mivel lényegesen több bemenet feldolgozására képes, a mély tanulás pontosabban tudja megjósolni a mai fenyegetéseket, miközben folyamatosan naprakész marad.

Könnyebb: A hagyományos gépi tanulási megközelítések hatalmas modellméretekkel járnak, és olykor sok gigabájtot foglalnak el a lemezen. A Sophos mély tanulási megközelítése azonban jelentős mértékben tömörített modelleket eredményez. A Sophos mély tanulási modellje rendkívül kisméretű, a végponton kevesebb mint 20 MB-ot foglal, és szinte egyáltalán nincs hatással a teljesítményre.

A Sophos mély tanulási képességei

A Sophos az iparág legjobban teljesítő kártevőészlelő motorjának köszönhetően mély tanulási szakértelmet nyújt:

Tapasztalt: Versenytársainkkal ellentétben mi sokéves tapasztalattal rendelkezünk számítógépes biztonsági és gépi tanulási szakértőkként, és kártevőészlelő mély tanulási modelljeink évek óta működnek éles környezetben. A Sophos kártevőészlelő modellt adatszakértőkből álló csapatunk DARPA alapú technológiával fejlesztette ki. 2010-ben az Egyesült Államok fejlett védelmi kutatási projekteket végző ügynöksége (Defense Advanced Research Projects Agency, DARPA), saját számítógépes genomprogramot hozott létre, hogy felfedje a kártevők és egyéb számítógépes fenyegetések „DNS-ét". Innen ered a jelenleg az Intercept X-be ágyazott algoritmus.

Kipróbált: Modelljeink mindig is nyitottak és átláthatók voltak. Módszertanunk olyan iparági konferenciákon történő bemutatásán felül, mint a Black Hat, attól sem hátráltunk meg, hogy harmadik feleknek engedjük meg modellünk tesztelését. Ez a modell 2016 augusztusa óta bizonyít a VirusTotalon, és magas pontszámot kapott olyan független tesztelőktől, mint az NSS Labs. Minden esetben rendkívül hatékonynak bizonyult, miközben kevés hamis pozitívot eredményezett.

„A tesztjeink során valaha látott egyik legjobb teljesítménypontszám"

Maik Morgenstern, műszaki igazgató, AV-TEST

Teljesítmény: A Sophos mély tanulási technológiája rendkívül gyors. A modell kevesebb mint 20 milliszekundum alatt képes több millió tulajdonságot kivonni egy fájlból, mély elemzést végezni, és megállapítani, hogy a fájl jó- vagy rosszindulatú. Ez az egész folyamat a fájl végrehajtása előtt történik.

SophosLabs: Bármely modell egyik legfontosabb kelléke a tanulásra használt adathalmaz. Adatszakértői csapatunk a SophosLabsben dolgozó csoport része, és több millió mintához férhet hozzá. Ez lehetővé teszi számukra, hogy modelljeinkben a lehető legjobb előrejelzéseket biztosítsák. A két csoport közötti integráció ugyanakkor jobb adatcímkézést (és ezáltal jobb modellezést) is eredményez. A fenyegetéssel kapcsolatos információk, valamint az adatszakértőinkhez és fenyegetéskutatóinkhoz a valós világból érkező visszajelzések kétirányú megosztása folyamatosan javítja modelljeink pontosságát.

„Az Intercept X minden bonyolult és speciális támadást megakadályozott, amivel próbára tettük."

ESG laboratóriumi jelentés, 2017. december

Próbálja ki most ingyen

Regisztráljon a 30 napos, ingyenes próbára a sophos.com/interceptx oldalon

Sales Eastern Europe
Email: salesee@sophos.com

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

SOPHOS