SOPHOS
Security made simple.

Intercept X Deep Learning

Intercept X kombinuje hloubkové učení s prvotřídní technologií zajišťující ochranu proti útokům, technologií CryptoGuard pro ochranu před ransomwarem, analýzou prvotních příčin a mnoha dalšími technologiemi, které tvoří nejkomplexnější ochranu koncových bodů na trhu. Tato jedinečná kombinace funkcí umožňuje produktu Intercept X zastavit nejrůznější hrozby pro koncové body.

Přednosti

- Nejlépe fungující engine pro detekci malwaru
- Chrání nejen před známými, ale i dosud nevídanými druhy malwaru
- Blokuje malware ještě před tím, než se spustí
- Nezávisí na podpisech
- Chrání i tehdy, když je hostitelský počítač offline
- Odhalí malware přibližně za 20 milisekund
- Vyškolen na stovkách miliónů vzorků
- Od srpna 2016 se osvědčuje na stránce VirusTotal
- Klasifikuje soubory jako škodlivé, potenciálně nechtěné aplikace (PUA) či neškodné
- Funguje ihned po nasazení a nevyžaduje žádné další školení
- Velmi malá velikost (méně než 20 MB)
- Zaměřený na Windows Portable Executable

Spousta dnešních bezpečnostních řešení je reaktivní a příliš pomalá. Objem a složitost útoků na koncové body stále roste a starší koncepce mají problém držet s nimi krok. Například společnost SophosLabs každý den zanalyzuje více než 400 000 nových vzorků malwaru. A aby bylo řešení tohoto problému ještě obtížnější, společnost SophosLabs navíc odhalila, že 75 % malwaru je specifických pro jedinou organizaci.

Deep learning, pokročilá forma strojového učení, pomáhá měnit náš přístup k ochraně koncových bodů a Intercept X je v této oblasti lídrem. Díky tomu, že Intercept X využívá deep learning, mění ochranu koncových bodů z reaktivní na prediktivní metodu, a dokáže tak ochránit i před neznámými hrozbami.

Deep Learning vs. jiné typy strojového učení

„Intercept X funguje na bázi neuronové sítě hloubkového učení, která pracuje podobně jako lidský mozek... Výsledkem je vysoká přesnost jak u existujícího, tak i zero-day malwaru a nižší výskyt falešných poplachů."

Zpráva ESG Lab, prosinec 2017

Přestože mnoho produktů o sobě tvrdí, že využívá strojové učení, nejsou všechny jeho typy tvořeny stejně. My ve společnosti Sophos používáme k odhalení malwaru hloubkové učení. Hloubkové učení, označované také jako „neuronové sítě hloubkového učení" či „neuronové sítě", se inspirovalo způsobem, jakým funguje lidský mozek. Jedná se o stejný typ strojového učení, kterého se často využívá k rozpoznávání obličejů, zpracovávání přirozeného jazyka nebo u samořízených aut a v dalších pokročilých oborech počítačové vědy a výzkumu.

Deep learning neustále překonává jiné modely strojového učení, například náhodný les, shlukování k-means nebo Bayesovské sítě, ale vytvoření účinného modelu vyžaduje obrovské množství dat a velký výpočetní výkon. Tento proces však byl ve společnosti Sophos usnadněn díky sběru malwaru, který v minulých 30 letech společnost SophosLabs prováděla a na jehož analýzu vynaložila velké úsilí, a také telemetrii, kterou každý den obdržíme od více než 100 miliónů koncových bodů.

Deep learning má několik podstatných výhod v porovnání s jinými typy strojového učení běžně používanými pro ochranu koncových bodů:

Chytřejší: Modely hloubkového učení zpracovávají data podobně jako neurony v lidském mozku přes více analytických vrstev a každá taková vrstva dělá model značně silnějším. Analyzuje spletité spojitosti mezi různými vstupními vlastnostmi. To mu umožňuje automaticky odhalit nejlepší kombinaci a zacházení se vstupy, které by jinak pro člověka bylo nemožné určit. To znamená, že model hloubkového učení pro detekci malwaru Sophos bude schopen odhalit malware, kterého by si jiné enginy na bázi strojového učení nevšimly.

Více škálovatelný: Deep Learning se elegantně škáluje na stovky miliónů výukových vzorků. To je velmi důležité, vezmeme-li v úvahu, že společnost SophosLabs každý týden analyzuje 2,8 miliónu nových vzorků malwaru. Díky tomu, že náš model dokáže neustále hltat obrovské množství výukových dat, zvládne se „naučit" celé pozorovatelné prostředí hrozeb jako část svého školicího procesu. A jelikož je hloubkové učení schopno zpracovávat podstatně větší množství vstupních dat, dovede ještě přesněji předpovídat hrozby v současnosti a přitom zůstávat aktuální v průběhu času.

Menší velikost: Běžné koncepce strojového učení mají za následek ohromnou velikost modelu, který často zabírá i několik gigabytů na disku. Naproti tomu koncepce hloubkového učení Sophos vede k velké komprimaci modelů. Tento model hloubkového učení je neuvěřitelně malý, jeho velikost na koncovém bodě je menší než 20 MB, a nemá prakticky žádný dopad na výkon.

Schopnosti hloubkového učení Sophos

Společnost Sophos poskytuje odborné znalosti hloubkového učení s nejvýkonnějším enginem pro detekci malwaru v oboru:

Zkušenosti: Na rozdíl od konkurence jsme již dlouhou dobu odborníky v oblasti strojového učení využívaného pro kybernetickou bezpečnost a už mnoho let produkujeme modely hloubkového učení pro detekci malwaru. Model pro detekci malwaru Sophos byl vytvořen naším týmem vědců využívajícím technologii poskytnutou agenturou DARPA. V roce 2010 vytvořila Agentura ministerstva obrany Spojených států amerických pro pokročilé výzkumné projekty (DARPA) program Cyber Genome, jehož úkolem bylo odhalit „DNA" malwaru a dalších kybernetických hrozeb. Ten se stal počátkem toho, co je nyní algoritmus zabudovaný do Intercept X.

Osvědčenost: V případě našich modelů jsme vždy otevření a transparentní. Nejenže na odvětvových konferencích, jako třeba Black Hat, prezentujeme detaily naší metodiky, ale také se nestydíme umožnit nezávislým třetím stranám testovat náš model. Model se také už od srpna 2016 osvědčuje na stránce VirusTotal a získal vysoká hodnocení od testerů třetích stran, například NSS Labs. V každém případě se osvědčil svou vysokou účinností a nízkým počtem falešných poplachů.

„Jedno z nejlepších výkonnostních skóre, jaké jsme kdy v našich testech viděli."

Maik Morgenstern, technický ředitel, AV-TEST

Výkon: Technologie hloubkového učení společnosti Sophos je neskutečně rychlá. Model je schopen za necelých 20 milisekund extrahovat ze souboru milióny vlastností, provést důkladnou analýzu a určit, zda je soubor bezpečný nebo škodlivý. Celý tento proces proběhne ještě předtím, než se soubor spustí.

SophosLabs: Jedním z nejdůležitějších aspektů jakéhokoli modelu jsou data použitá na vyškolení. Náš tým vědců je součástí skupiny SophosLabs, která jim dává přístup ke stovkám miliónů vzorků. To jim umožňuje vytvořit modely schopné těch nejlepších předpovědí. Integrace těchto dvou skupin také vede k lepšímu označování dat (a tedy i k lepšímu modelování). Obousměrné sdílení inteligence hrozeb a zpětné vazby z reálného světa mezi týmem vědců a výzkumníky hrozeb neustále zvyšuje přesnost našich modelů.

„Intercept X zastavil každý komplikovaný, pokročilý útok, který jsme proti němu poslali."

Zpráva ESG Lab, prosinec 2017

Vyzkoušejte si řešení zdarma

Zaregistrujte se na adrese sophos.com/interceptx a vyzkoušejte produkt na 30 dní zdarma.

Obchodní zastoupení pro východní Evropu
E-mail: salesee@sophos.com

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

SOPHOS