Simovits Consulting AB
Saltmätargatan 8A
113 59 Stockholm
mikael@simovits.com

Maskininlärningsbaserat system för bedömning av cyberattacker

Bakgrund

Som inom många andra områden har de senaste decenniets framsteg inom AI, och närmare bestämt maskininlärning, haft en direkt inverkan på IT-säkerhetssektorn. Automatiska filter för exempelvis skräpmeddelanden har gått från att använda simpla maskininlärningsmetoder till att använda djupinlärningsmodeller som ofta har väldigt hög noggrannhet. Antivirussystem har på samma sätt gått bortom simpel signatur baserad detektion till att använda molnbaserade maskininlärningsmetoder. Parallellt med denna utveckling av avancerade skyddsmekanismer har många förövare riktat in sig på andra områden, där ett framträdande är nätfiske. Konsekvenser av framgångsrika nätfiske-attacker kan ofta vara förödande. Skyddsmekanismer mot nätfiske är nästan alltid inriktade på att skydda användare utan dennas vetskap. Allt som inte fångas av dessa skyddsmekanismer måste då utan stöd hanteras av användaren, vilket gör att till och med framträdande säkerhetsorganisationer har blivit drabbade av intrång till följd av nätfiske då deras icke-säkerhetspersonal saknar referenserna och kunskapen för att kunna bedöma skadliga epost och länkar. Trots ett system med en hög noggrannhet kommer därför visst nätfiske förbli odetekterad, dock med liten marginal. Lösningar som kan assistera användare i att bedöma skadligt innehåll, så som webblänkar (URL:er) och avsändaradresser, är därför något som kan hjälpa för att bemötta denna ökande tendens av nätfiske samt dessa fall som ej plockas upp av nuvarande metoder.

Ihop med stödet ovan så finns det flera sätt som nuvarande systems kan bli bättre trots deras överlag höga effektivitet. Nuvarande lösningar är oftast djupt integrerade i stora och kommersiella produkter som ofta är molnbaserade vilket erfordrar att organisationen delar med sig av sin data till en tredje-part. Detta innebär att förmågan att kunna få insyn i dessa lösningar och skräddarsy de efter en viss situation är begränsad. Vidare går det heller inte ofta att återanvända och dela information mellan olika lösningar som annars analyserar likartad data. En lösning som bemöter dessa aspekter kännetecknas av:

- *Transparent* – Både säkerhetspersonal och vanliga användare ska kunna få en förståelse av hur lösningen har bedömt en given datapunkt. Detta innebär exempelvis att den sammantagna bedömningen redovisas ihop med explicita sannolikheter resulterande ifrån de olika moduler (se nedan) och den totala beräknade sannolikheten för klassificeringen. Andra faktorer, så som använd träningsdata, bör likaså kunna presenteras.
- *Modulärt* – Lösningen ska kunna använda sig av flera olika modeller (s.k ensemble-inlärning) för klassificering som fokuserar på samma eller olika delar av datakällan. Utifrån de olika klassificeringarna ska en total bedömning kunna formas, som generellt kan vara ett viktat medelvärde beroende på modulernas bedömda tillförlitlighet. Moduler ska kunna återanvändas för fall då informationen är likartad och då åtnjuta fördelarna med tidigare inlärning. Alla modulerna behöver inte utgå ifrån maskininlärning och kan istället ta hänsyn till Open source intelligence-källor.

Simovits Consulting AB
Saltmätargatan 8A
113 59 Stockholm
mikael@simovits.com

- *Flexibelt* – Lösningen ska ha ett lättillgängligt applikationsgränssnitt (API) som gör att många olika tjänster kan integrera med denna. Genom att frikoppla själva maskininlärningslösningen ifrån det sammantagna systemet blir det möjligt att använda denna i flera olika sammanhang och även att ha en centrallösning inom organisationen. Några exempel kan vara logganalys, webbplugin, webbfilter eller en dedikerad användarwebbtjänst i still med VirusTotal.

Utifrån dessa punkter kan en lösning upprättas som på ett mer rättframsätt kan kombineras med mänsklig intuition för att fatta en slutgiltig bedömning och fungera som stöd både för säkerhetspersonal och för vanliga användare för att på sådant sätt reducera risken för exempelvis skadliga webbsidor och/eller epost.

Examensarbete

Avsikten med examensarbetet är att utveckla en första versionen av en lösning som behandlar ovanstående punkter. Du ges själv stora möjlighet att utforma lösningen och hur den uppfyller punkterna ovan. Bland annat har du helt fria händer att välja vad för maskininlärningsmodeller som används i de olika modulerna. En möjlig utgångspunkt är en lösning som kan bedöma/klassificera skadliga källor som representeras av olika strängar med likartade delar, vilket bland annat innefattar URL:er och epost-adresser. Modulerna kan undersöka dessa i olika faser. Först betraktas de olika delarna av strängarna (i exemplet ovan URL:ernas olika delar och epost-adressens domän samt lokala namn) och sedan kan dynamiska analyser ske av källan om detta är möjligt (så som undersökning av http svarshuvuden ifrån den berörda webbsidan). Ett system som använder sig av denna lösning kan sedan vara en simpel webbapplikation som tar emot en datakälla enligt ovan och sedan presenterar de relevanta resultaten för användaren så att denna kan fatta ett slutgiltigt beslut om URL:en eller epost-adressens skadlighet. Framtida vidarebyggning av lösningen, så som avvikelsedetektering i nätverkstrafik, kan sedan utgå ifrån denna första versionen utifrån nya moduler.

Vi förutsätter inga kunskaper inom IT-säkerhet men ser gärna att du har någon erfarenhet av maskininlärning och programmering, exempelvis ifrån någon kurs eller ifrån ett projekt.

Om företaget

Simovits Consulting AB är ett Stockholmsbaserat konsultföretag inom Informations- och cybersäkerhet. Vi är ett femtontal konsulter som arbetar med korttidsuppdrag som spänner från allt mellan penetrationstest och forensiska undersökningar till etablering av ledningssystem och informationskartläggningar. Avsikten med examensarbetet är att utgöra en del i företagets forskning och omvärldsbevakning, men framförallt för dig att känna på vad ett typiskt uppdrag kan innebär och för oss att på sikt hitta en ny kollega.

Simovits Consulting AB
Saltmätargatan 8A
113 59 Stockholm
mikael@simovits.com

Ansök

Skicka ansökan tillsammans med betygsutdrag och en kortfattad beskrivning av dig själv till:

Mikael Simovits
070-741 51 62
mikael@simovits.com