**PERSBERICHT**

**Nieuwste versie van Sophos’ Intercept X:**

**Predictive protection met geavanceerde deep learning**

*Effectiever dan traditionele machine learning: deep learning geeft Sophos Intercept X de hoogste detectiepercentages en laagste false positives in de markt voor next-generation endpoint security*

Oosterhout, 30 januari 2018 - **Sophos lanceert Intercept X met malwaredetectie, die wordt ondersteund door geavanceerde *deep learning* neurale netwerken. Gecombineerd met nieuwe active hacker mitigaties, geavanceerde applicatievergrendeling en verbeterde ransomwarebescherming levert deze nieuwste versie van de next-generation endpointbeveiliging ongekende detectie- en preventieniveaus.**

*"Predictive Protection**is de toekomst van IT-beveiliging. Sophos heeft een enorme stap voorwaarts genomen door deep learning neurale netwerken aan Intercept X’s exploit- en ransomwarebescherming toe te voegen”,* zegt Dan Schiappa, Senior Vice President en General Manager Producten bij Sophos. “*In staat zijn om te beschermen tegen aanstaande, onbekende aanvallen in plaats van te wachten tot deze daadwerkelijk toeslaan, zal de manier zijn waarop IT-activiteiten in elke organisatie hun gebruikers en eigendommen kunnen beschermen drastisch veranderen. Intercept X biedt de meest geavanceerde bescherming van de toekomstige generaties - voor elke organisatie, ongeacht hun strategie.”*

De belangrijkste nieuwe functies binnen Intercept:

***Deep Learning Malware Detection***

* Deep learning-model spoort bekende en onbekende malware op en potentieel ongewenste toepassingen (PUA’s) voordat ze worden uitgevoerd, zonder op handtekeningen te vertrouwen
* Het model is minder dan 20MB en vereist niet telkens een update

***Active Adversary Mitigations***

* Bescherming tegen ontvreemding van (persoons)gegevens - voorkomt diefstal van authenticatiewachtwoorden en hash-informatie uit geheugen en permanente opslag
* Code cave utilization - detecteert de aanwezigheid van codes die in een andere applicatie worden gebruikt (vaak gebruikt ter vermijding van antivirus)
* APC-bescherming - spoort het misbruik van Asynchronous Procedure Calls (APC) op dat vaak wordt gebruikt als onderdeel van de AtomBombing-code injectietechniek en recentelijk meer gebruikt als de methode voor het verspreiden van de WannaCry-worm en NotPetya-wisser via EternalBlue en DoublePulsar.

***Nieuwe en verbeterde Exploit Prevention Techniques***

* Schadelijke procesmigratie - detecteert DLL-injectie die door kwaadwillenden wordt gebruikt om te schakelen tussen processen die op het systeem worden uitgevoerd
* Process Privilege Escalation - voorkomt dat een low-privilege proces wordt opgeschaald naar een hoger privilege; het is een tactiek die wordt gebruikt om een ​​verhoogde systeemtoegang te verkrijgen.

***Verbeterde Application Lockdown***

* Vergrendeling van browsergedrag - Intercept X voorkomt het kwaadwillige gebruik van PowerShell van browsers als een standaard bahavior lockdown
* Vergrendeling van de HTA-applicatie - HTML-applicaties die door de browser worden geladen, zullen de lockdown-beperkende maatregelen worden toegepast (alsof ze een browser zijn).

Deep learning is de nieuwste ontwikkeling van machine learning en levert een zeer schaalbaar detectiemodel dat in staat is het gehele waarneembare dreigingslandschap te leren kennen. Met het vermogen om honderden miljoenen samples te verwerken, kan deep learning nauwkeuriger voorspellingen maken met een hoger percentage met veel minder false positives in vergelijking met traditionele machine learning.

De nieuwste versie van Sophos Intercept X bevat niet alleen innovaties op het gebied van anti-ransomware en exploitpreventie, maar ook actieve mitigatiemetingen zoals bescherming tegen diefstal van inloggegevens. Omdat antimalware is verbeterd, zijn aanvallen steeds meer gericht op het stelen van inloggegevens om vervolgens als ‘legitieme gebruiker’ op en rond systemen en netwerken te kunnen bewegen. Intercept X detecteert dit gedrag en voorkomt dit. Intercept X wordt via het cloud-gebaseerde beheerplatform Sophos Central geïnstalleerd en kan naast bestaande endpointbeveiligingssoftware van veel leveranciers worden geïnstalleerd. Hierdoor wordt endpointbeveiliging direct verbeterd. In combinatie met Sophos XG Firewall kan Intercept X gesynchroniseerde beveiligingsmogelijkheden introduceren om bescherming nog meer te optimaliseren.

Intercept X werd voor het eerst in september 2016 gelanceerd en heeft zijn weg naar tienduizenden organisaties over de hele wereld al weten te vinden.
Voor meer informatie: [www.sophos.com/interceptx](http://www.sophos.com/interceptx).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Sandra Van Hauwaert, sandra@square-egg.be, GSM 0497 251816

**Over Sophos**
Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com).