Persbericht

**Sophos versterkt
Intercept X for Server with Endpoint Detection and Response**

*Nieuwe toevoeging helpt bedrijven bij het bestrijden van nieuwe ‘blended’ cyberaanvallen*

Brussel, 3 juni 2019 - **Sophos introduceert Intercept X for Server with Endpoint Detection and Response (EDR). Door EDR aan Intercept X for Server toe te voegen, zijn IT-managers in staat cyberaanvallen te onderzoeken tegen servers die een gewild doelwit blijken vanwege de data die daar staan opgeslagen. Cybercriminelen evolueren hun methoden en combineren nu automatisering en menselijke hacking-activiteiten om aanvallen op servers succesvol te kunnen uitvoeren. Deze nieuwe ‘blended’ aanvalsmethodiek combineert het gebruik van bots om potentiële slachtoffers te identificeren met personen achter een toetsenbord die beslissingen nemen over wie (en hoe) aan te vallen.**

Het SophosLabs Uncut-artikel [Worms Deliver Cryptomining Malware to Web Servers](https://news.sophos.com/en-us/2019/05/30/worms-deliver-cryptomining-malware-to-web-servers/) onderstreept hoe gemakkelijk het voor cybercriminelen is om bots in te zetten en ‘soft targets’ te ontdekken. In het rapport wordt een geautomatiseerde aanval uitgelegd die een breed scala aan kwaadaardige codes kan genereren voor servers die achterlopen met updatecycli.

**Blended Cyberattack: een anatomie**

Zodra de bots potentiële doelen hebben geïdentificeerd, gebruiken cybercriminelen hun kennis om slachtoffers te selecteren op basis van onder meer gevoelige gegevens, intellectueel eigendom, het vermogen om losgeld te betalen of toegang tot andere servers en netwerken te geven. De laatste stappen vinden handmatig en doordacht plaats: inbreken, detectie ontwijken en lateraal bewegen om zo toe te slaan, rondsluipen, intelligentie stelen en ongemerkt weer weggaan, back-ups uitschakelen en servers versleutelen om zo losgeld te vragen en slachtoffers gebruiken als lanceerplatforms om andere bedrijven aan te vallen: het zijn slechts voorbeelden van hoe zij te werk kunnen gaan.

“Blended cyberaanvallen worden een alledaagse activiteit voor cybercriminelen omdat ze winstgevend zijn”, zegt Dan Schiappa, productmanager Sophos. “De meeste malware is nu geautomatiseerd, dus het is gemakkelijk voor aanvallers om organisaties met zwakke beveiliging te vinden, hun betaalpotentieel te evalueren en *hand to keyboard*-hacktechnieken te gebruiken om zoveel mogelijk schade aan te richten.”

**Sophos Intercept X for Server with EDR**

Met Sophos Intercept X for Server with EDR hebben IT-managers, ongeacht de bedrijfsgrootte, vanaf vandaag maximale zichtbaarheid. Hierdoor kunnen ze sluipende aanvallen proactief opsporen, de impact van beveiligingsincidenten beter begrijpen en snel rapporteren over wat er wel (of niet) heeft plaatsgevonden.

“Wanneer criminelen een netwerk binnendringen, gaan ze in een rechte lijn op servers af. Helaas houden veel organisaties er een conservatieve benadering op na wanneer het op wijzigingen aankomt, waardoor patching vaak vertraging oploopt. In feite rekenen cybercriminelen op deze vertraging. Wanneer organisaties slachtoffer worden van een aanval, moeten ze precies weten wat, hoe en wanneer apparaten en servers zijn geraakt om vervolgens vragen te beantwoorden op basis van strengere regelgeving. Door deze informatie de eerste keer nauwkeurig in kaart te brengen, kunnen bedrijven problemen sneller oplossen en toekomstige *breaches* voorkomen”, aldus Schiappa.

Sophos Intercept X for Server with EDR breidt Sophos' aanbod van EDR uit, die voor het eerst voor Intercept X for Endpoint in oktober 2018 werd aangekondigd. EDR wordt ondersteund door *deep learning*-technologie om malware op te sporen. Sophos’ diepgaande neurale netwerk wordt getraind op honderden miljoenen samples om verdachte kenmerken van schadelijke codes op te sporen en zo nog nooit eerder waargenomen bedreigingen te detecteren. Het biedt een brede, deskundige analyse van mogelijke aanvallen door het DNA van verdachte bestanden te vergelijken met de malware-voorbeelden die al in SophosLabs zijn gecategoriseerd.

Met Sophos EDR hebben IT-managers ook *on-demand* toegang tot informatie van SophosLabs, onderzoeken naar verdachte gebeurtenissen en een aanbevolen stappenplan. Om volledig zicht te houden op het dreigingslandschap, traceert, deconstrueert en analyseert SophosLabs elke dag 400.000 unieke en voorheen onbekende malwareaanvallen.

**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).

Voor meer informatie:

Square Egg Communications, Sandra Van Hauwaert, sandra@square-egg.be, GSM 0497251816.