**PERSBERICHT**

**"Cybercriminelen vallen binnen 52 seconden cloudserver-honeypots aan "**

**Brussel, 9 april 2019 - Slechts 52 seconden nadat een honeypot in Sao Paulo live ging, werd deze al door cybercriminelen aangevallen. Het is een van de bevindingen van Sophos’ onderzoek** [**Exposed: Cyberattacks on Cloud Honeypots**](http://www.sophos.com/CloudHoneypotsReport)**. Een honeypot is een systeem dat vermoedelijke doelen van cyberaanvallen nabootst, zodat onderzoekers het gedrag van cybercriminelen kunnen volgen. Gemiddeld werd er dertien keer per minuut een poging gedaan de onderzochte cloudserver-honeypots aan te vallen.**

Sophos nam een maand lang tien cloudserver-honeypots onder de loep, opgezet in populaire AWS-datacentra in Californië, Frankfurt, Ierland, Londen, Mumbai, Ohio, Parijs, Sao Paulo, Singapore en Sydney. In die periode werden er meer dan vijf miljoen aanvalspogingen op het wereldwijde honeypotnetwerk gedaan. Gemiddeld werden de tien cloudserver-honeypots binnen veertig minuten door cybercriminelen aangevallen. De studie van Sophos demonstreert hoe cybercriminelen automatisch op zwakke open cloud buckets scannen. Bij een succesvolle aanval kunnen organisaties slachtoffer worden van datalekken. Cybercriminelen gebruiken daarnaast deze ‘breached’ cloudservers om tot andere servers of netwerken toegang te krijgen.

Matthew Boddy, securityspecialist bij Sophos, licht toe: "Het onderzoek laat zien met welke bedreigingen organisaties te maken krijgen wanneer ze overstappen naar hybride en all-cloudplatforms. De snelheid en schaal van aanvallen op de honeypots tonen aan hoe meedogenloos en volhardend cybercriminelen zijn. Ze gebruiken botnets om zich te richten op de cloudplatforms van organisaties. In sommige gevallen kan de aanvaller ook een mens zijn, maar bedrijven hebben hoe dan ook een beveiligingsstrategie nodig om alles wat ze in de cloud zetten te beschermen. Het probleem van zichtbaarheid en beveiliging op cloudplatforms blijft een uitdaging, zeker nu het gebruik van de cloud toeneemt."

**Zichtbaarheid op zwakheden**

Om te weten welke data precies beschermd moeten worden is continue zichtbaarheid van de publieke cloudinfrastructuur voor bedrijven van vitaal belang. Tegelijkertijd maken meerdere ontwikkelteams binnen een organisatie en een steeds veranderende, *auto-scaling* omgeving die zichtbaarheid een serieus probleem voor IT-beveiliging. Sophos pakt deze beveiligingszwakte in openbare clouds aan met de lancering van Sophos Cloud Optix, ​​die kunstmatige intelligentie toepast voor betere cloudinfrastructuur, compliance en threat response in meerdere cloudomgevingen.

Ross McKerchar, CISO bij Sophos, voegt toe: “In plaats van het overladen van securityteams met ongedifferentieerde alerts minimaliseert Sophos Cloud Optix de ‘alertmoeheid’ door te identificeren wat belangrijk is en waarop actie moet worden ondernomen. Door het toevoegen van zichtbaarheid in cloud assets en workloads krijgt IT-security een veel beter beeld van hun securityprioriteiten die door Sophos Clous Optix worden aangegeven.”

**De voornaamste kenmerken van Sophos Cloud Optix:**

*Slimme zichtbaarheid*

Automatische opsporing van de bedrijfsmiddelen van een organisatie in AWS-, Microsoft Azure- en Google Cloud Platform-omgevingen. Werkt via één console, waardoor beveiligingsteams zicht hebben op alle data in de cloud en binnen enkele minuten kunnen reageren en herstellen.

*Continue Cloud Compliance*

Blijft up-to-date met voortdurend veranderende compliance door veranderingen in cloud-omgevingen automatisch te detecteren.

*AI-gebaseerde monitoring en analyses*

Verlaagt respons- en oplossingstijden van incidenten van dagen/weken naar slechts enkele minuten. De krachtige AI detecteert risicovolle resource configuraties en verdacht netwerkgedrag met slimme waarschuwingen en optionele automatische risicosanering.

Sophos Cloud Optix maakt gebruik van Avid Secure’s AI-technologie. Dit bedrijf werd in januari 2019 door Sophos overgenomen. Avid Secure werd in 2017 opgericht door een team van vooraanstaande leiders uit de IT-beveiliging en heeft een revolutie teweeggebracht in de beveiliging van openbare cloud-omgevingen door effectieve end-to-end bescherming te bieden in cloudservices (zoals AWS, Azure en Google).

Voor het volledige rapport [Exposed: Cyberattacks on Cloud Honeypots](http://www.sophos.com/CloudHoneypotsReport) en het bijbehorende artikel [Naked Security](https://nakedsecurity.sophos.com/cloudhoneypots).

**Voor meer informatie, contacteer:**

Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.

**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).