**Media Alert**

**Sophos 2020 Threat Report gaat in op voornaamste cyberattacks**

*Rapport toont aan hoe cyberaanvallen op ransomware inzetten, onder de radar blijven met kwaadaardige Android-apps, misbruik maken van misconfiguratie in de cloud en misbruik maken van machine learning*

Oosterhout, 5 november 2019 – **In het** [**2020 Threat Report**](https://www.sophos.com/en-us/threatreport2020.aspx) **van Sophos dat vandaag is gelanceerd, wordt ingegaan op het snel evoluerende landschap van cyberdreigingen. Het rapport laat zijn licht schijnen op de ontwikkelingen van de laatste twaalf maanden, maar kijkt ook vooruit op de trends die in 2020 cybersecurity zullen beïnvloeden.**

“Het dreigingslandschap blijft zich ontwikkelen, en de snelheid en omvang van deze evolutie is zowel versnellend als onvoorspelbaar”, zegt John Shier, senior security advisor bij Sophos. “De enige zekerheid die we hebben, is wat er op dit moment gebeurt. Daarom kijken we in ons Threat Report 2020 naar de invloed van bestaande trends voor het komende jaar. We benadrukken hoe kwaadwillenden steeds meer onder de radar opereren, steeds vernuftiger worden met het exploiteren van fouten, hun activiteiten goed verborgen houden en detectietechnologieën ontwijken - in de cloud, via mobiele apps en binnen netwerken. Het Threat Report 2020 is niet zozeer een plan, maar kan worden gezien als wegbewijzering om zo beter te begrijpen wat de komende periode in petto heeft en hoe bedrijven zich optimaal kunnen voorbereiden.”

Het Threat Report richt zich op zes gebieden waarin researchers in het afgelopen jaar bijzondere ontwikkelingen hebben opgemerkt. Hieronder bevinden zich ook ontwikkelingen die naar verwachting een significante impact hebben op het landschap van cyberdreigingen in 2020:

**Ransomware-aanvallers verhogen de inzet met automated active attacks (AAA).** Op deze manier worden vertrouwde managementtools van organisaties tegen henzelf gekeerd, beveiligingscontroles ontweken en back-ups uitgeschakeld. Dit alles om de maximale impact in een zo kort mogelijk tijd te veroorzaken.

**Ongewenste apps komen dichter bij malware**. In het jaar van de Android Fleeceware-apps en meer bijna onzichtbare en agressieve adware belicht het Threat Report hoe deze en andere potentially unwanted apps (PUA), zoals browserplug-ins, tussenpersonen worden voor het leveren en uitvoeren van malware en bestandloze aanvallen.

**De grootste kwetsbaarheid voor cloud computing is een misconfiguratie door operators**. Naarmate cloudsystemen complexer en flexibeler worden, vormen operatorfouten een groeiend risico. In combinatie met een algemeen gebrek aan zichtbaarheid maakt dit cloud computing-omgevingen een kant-en-klaar doel voor cyberaanvallen.

**Machine learning, ontworpen om malware te tackelen, wordt zelf aangevallen**. 2019 was het jaar waarin het potentieel van aanvallen op machine learning beveiligingssystemen werd benadrukt. Onderzoek heeft aangetoond hoe detectiemodellen voor machine learning mogelijk kunnen worden misleid, en hoe machine learning kan worden toegepast om zeer overtuigende nepinhoud voor social engineering te genereren. Tegelijkertijd passen verdedigers machine learning toe op taal om kwaadaardige e-mails en URL’s te detecteren. Verwacht wordt dat dit geavanceerde kat en muisspel in de toekomst vaker zal voorkomen.

Andere gebieden in het rapport zijn onder meer het gevaar om cybercriminele verkenningen mis te lopen, het voortdurend uitbreidende aanvalsgebied van Remote Desktop Protocol (RDP) en de verdere opmars van Automated Active Attacks (AAA).

Meer informatie over het SophosLabs 2020 Threat Report is ook te vinden op <https://www.sophos.com/en-us/threatreport2020.aspx> en <https://nakedsecurity.sophos.com/>

**Over Sophos**

Als wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen. Aangedreven door SophosLabs, een wereldwijd team voor *threat intelligence* en *data science*, beschermen de cloudgebaseerde en AI-aangedreven oplossingen laptops, servers, mobiele devices en netwerken tegen immer evoluerende cyberaanvaltechnieken waaronder ransomware, malware, exploits en phishing.

Het cloudgebaseerde beheerplatform Sophos Central integreert het volledige portfolio van Sophos’ *next-gen* oplossingen (waaronder de endpointoplossing Intercept X en XG next-gen firewall) in een enkel ‘gesynchroniseerd beveiligingssysteem’ dat via een set API's toegankelijk is. Sophos verkoopt zijn oplossingen en diensten via een wereldwijd kanaal van meer dan 47.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën via Sophos Home ook beschikbaar aan consumenten. Het bedrijf heeft zijn hoofdkantoor in Oxford (VK) en wordt op de London Stock Exchange onder het symbool *‘SOPH’* verhandeld. Voor meer informatie: [www.sophos.com](http://www.sophos.com).

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

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