**Media-alert**

**Sophos 2019 Threat Report:**

**De opkomst van gerichte cyberaanvallen en cybercriminelen die slachtoffers stalken om zo miljoenen op te halen**

Brussel, 14 november 2018 - **Vandaag lanceert Sophos zijn Threat Report 2019 waarmee het een uniek inzicht geeft in drie belangrijke cybersecuritytrends. Om tot dit inzicht te komen, hebben SophosLabs-onderzoekers het dreigingslandschap de afgelopen twaalf maanden onderzocht. Het rapport toont aan hoe deze cybersecuritytrends naar verwachting 2019 zullen beïnvloeden.**

“Het dreigingslandschap is zonder twijfel in beweging. Minder ontwikkelde cybercriminelen haken af, en de goede worden nog beter. Uiteindelijk zal er een kleine, doch sterke groep overblijven. Deze nieuwe cybercriminals zijn een kruising van de ‘targeted attacker’ van weleer en gebruikers van ‘off the shelf’ malware die handmatige hackingtechnieken gebruiken. Niet voor spionage of sabotage maar om er een meer dan goed inkomen aan over te houden.” - Joe Levy, CTO van Sophos.

Het SophosLabs 2019 Threat Report richt zich op deze voornaamste cybercrimeaanvallen (en hun gedrag):

**1/ Cybercriminelen wenden zich tot gerichte ransomware; inspiratie voor copycat-aanvallen**

In 2018 harkten cybercriminelen miljoenen dollars binnen met handgemaakte, gerichte ransomware-aanvallen. Deze interactieve, vooraf bestemde aanvallen zijn anders en schadelijker dan de ‘spray and pray’-achtige bot-aanvallen die automatisch worden verspreid via massale e-mails. Menselijke aanvallers kunnen slachtoffers vinden, lateraal denken, ‘wegversperringen overwinnen’ en back-ups verwijderen zodat er een hoge som losgeld moet worden betaald. Sophos gelooft dat het financiële succes van gerichte ransomware (SamSam, BitPaymer en Dharma) copycat-aanvallen inspireert en dat dit alleen meer zal toenemen in het komende jaar.

**2/ Cybercriminelen gebruiken reeds beschikbare Windows admin tools**

Het Threat-rapport onthult verder een verschuiving in de uitvoering van bedreigingen. Dit omdat steeds meer reguliere aanvallers hun technieken zodanig hebben ontwikkeld om gemakkelijk beschikbare IT-tools te gebruiken om door een systeem te gaan en hun missie te voltooien - of het nu gaat om het ontvreemden van gevoelige informatie van de server of het inzetten van ransomware.

*Admin tools worden cybercrime tools*

Een voorbeeld hiervan omvat een ironische draai, of Cyber ​​Catch-22: cybercriminelen maken gebruik van essentiële of ingebouwde Windows IT-admin tools, waaronder Powershell-bestanden en Windows Scripting-executables, om malware-aanvallen in te zetten.

*Cybercriminelen spelen ‘Digital Dominos’*

Door verschillende srcipttypes aan elkaar te koppelen die een aanval uitvoeren, kunnen hackers een kettingreactie initiëren voordat IT-managers een bedreiging op het netwerk detecteren. Eenmaal binnen is het moeilijk deze een halt toe te roepen.

*Nieuwere Office-exploits om slachtoffers te lokken*

Office-exploits zijn lange tijd een aanvalsvector geweest, maar onlangs hebben cybercriminelen oude exploits van Office-documenten door nieuwere vervangen.

*EternalBlue wordt belangrijk voor cryptojacking-aanvallen*

Patching updates verschenen meer dan een jaar geleden voor deze Windows-dreiging, maar de exploitatie van EternalBlue is nog steeds populair bij cybercriminelen; de koppeling van EternalBlue aan cryptomining-software verandert een hinderlijke hobby in een potentieel lucratieve criminele carrière. Door laterale distributie op bedrijfsnetwerken konden cryptojackers snel meerdere machines infecteren. Hierdoor krijgt de hacker meer uitbetaald en blijft de gebruiker met hoge kosten achter.

**3/ Mobiele en IoT-malware gaan ‘gewoon’ door**
Met de toename van illegale Android-apps is in 2018 steeds meer aandacht besteed aan malware voor telefoons, tablets en andere IoT-apparatuur. Aanvallers vinden alsmaar nieuwe manieren om detectie door Google te omzeilen en kwaadaardige apps binnen Play Market te krijgen.

Het complete Sophos 2019 Threat Report is terug te vinden op [www.sophos.com/threatreport](http://www.sophos.com/threatreport).

**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:**

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