**Sophos lanceert ‘Xstream’-versie van XG Firewall**
*Onderzoek Sophos Labs: “44% van cybercriminelen gebruikt encryptie om het kapen van data te verbergen.”*

**Oxford, 18 februari 2020** – Sophos introduceert de nieuwe "Xstream"-architectuur voor Sophos XG Firewall. Deze omvat onder meer Transport Layer Security (TLS)-decryptiemogelijkheden die beveiligingsrisico’s weghalen die zijn verbonden met versleuteld netwerkverkeer, veelal door securityteams over het hoofd gezien vanwege prestatie en complexiteit. XG Firewall biedt nu ook AI-verbeterde dreigingsanalyse van SophosLabs én versnelde applicatieprestaties.

Tevens heeft Sophos met ‘Nearly a Quarter of Malware now Communicates Using TLS’ een interessant rapport gepresenteerd. Hierin wordt aangegeven dat 23% van de malwarefamilies gecodeerde communicatie gebruikt voor Command and Control (C2) of installatie. Verder wordt ingegaan op veel voorkomende Trojaanse paarden (Trickbot, IcedID en Dridex) die tijdens aanvallen gebruikmaken van TLS. Cybercriminelen gebruiken TLS ook om hun exploits, payloads en gestolen data te verbergen en opsporing te voorkomen. Daarnaast gebruikt 44% van de cybercriminelen encryptie om gekaapte data te verbergen. Hieronder vallen onder meer bancaire en financiële inloggegevens en wachtwoorden, alsmede andere gevoelige data van andere organisaties.

Dan Schiappa, Chief Product Officer bij Sophos: "Cybercriminelen omarmen versleuteling om beveiligingsproducten te omzeilen. Helaas missen de meeste firewalls TLS-cryptomogelijkheden en zijn ze niet in staat om gecodeerd verkeer te inspecteren zonder dat applicaties netwerkprestaties binvloeden. Met de nieuwe Xstream-architectuur in onze XG Firewall bieden we inzicht in een enorme blinde vlek, terwijl onder meer compatibiliteitsproblemen worden opgelost met ondersteuning voor de TLS 1.3-standaard. Interne benchmarktests hebben een tweevoudige prestatieboost in de nieuwe XG TLS-inspectie aangetoond in vergelijking met eerdere XG-versies. Een ware *game changer*."

Vertraging weerhoudt IT-beheerders vaak van het gebruik van decodering, zoals te zien is in een onafhankelijk onderzoek onder 3.100 IT-managers in twaalf landen. De enquête ‘The Achilles Heel of Next-Gen Firewalls meldt dat hoewel 82% van de respondenten het erover eens was dat TLS-inspectie noodzakelijk is, slechts 3,5% van de organisaties dataverkeer decodeert voor inspectiedoeleinden.

**Belangrijke nieuwe functies van XG Firewall:**

* **Inspectie van TLS 1.3 om in SSL-stromen verstopte malware te detecteren**: De nieuwe port-agnostisch TLS-engine verdubbelt de performance bij crypto-operaties, vergeleken met vorige XG-versies.
* **Geoptimaliseerde performance van cruciale toepassingen**: Nieuwe FastPath policy controls versnellen de performance van SD-WAN toepassingen en netwerkverkeer, inclusief Voice over IP, Saas en anderen, tot de snelheid van een netwerkkabel.
* **Adaptive traffic scanning**: De nieuwe verbeterde Deep Packet Inspection (DPI) engine voert op netwerkverkeersstromen een dynamische risico-beoordeling uit en laat daar de bijbehorende threat scanning op los.
* **Dreigingsanalyse met informatie van SophosLabs**: Voorziet netwerkbeheerders van met behulp van de kunstmatige intelligentie van SophosLabs verbeterde dreigingsanalyse, om de verdediging te begrijpen en aan te passen, tegen een continu wijzigend dreigingslandschap.
* **Uitgebreid beheer en rapportage vanuit de cloud met Sophos Central**: Gecentraliseerde beheer- en rapportagemogelijkheden in Sophos Central voorzien klanten van groepsmatig firewall beheer en flexibele rapportagemogelijkheden, over een volledig bedrijfsnetwerk, zonder extra kosten.
* **Integratie met de Sophos Managed Threat Response (MTR) dienst**: XG Firewall klanten met een Sophos MTR Advanced abonnement hebben diepere, actiegerichte informatie om dreigingen te voorkomen, te detecteren, en erop te reageren, dankzij deze integratie.

**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:**

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