****

**Aanvalstechniek ‘Cloud Snooper’ laat malware via firewalls met elkaar communiceren**

**Brussel, BE - 26 februari 2020** – Sophos heeft een rapport over Cloud Snooper gepubliceerd, een geavanceerde aanvalstechniek die een unieke combinatie van technieken gebruikt om malware op servers toe te staan via firewalls vrij te communiceren met *command and control* servers. Het rapport ontleedt de tactieken, technieken en procedures (TTP's) die bij de aanvallen worden gebruikt. SophosLabs gelooft dat de aanval het werk was van een land met spionagedoeleinden.

De TTP’s omvatten een rootkit die firewalls omzeilt, een zeldzame techniek om toegang te krijgen tot servers die vermomd zijn als regulier verkeer én een backdoor-payload die schadelijke code deelt tussen zowel Windows- als Linux-besturingssystemen.

Hoewel elk element eerder bij aanvallen is waargenomen, zijn ze niet eerder in combinatie gezien. Sophos verwacht dat dit pakket van TTP's tot in de lagere

Rangen van de cybercriminele piramide zal doorsijpelen en als blauwdruk voor toekomstige firewallaanvallen zal dienen.

*“Dit is de eerste keer dat we een aanvalstactiek hebben gezien die een bypass-techniek combineert met een multiplatform payload, gericht op zowel Windows- als Linux-systemen. IT-securitysteams en netwerkbeheerders moeten snel heel veel werk verzetten met het patchen van alle externe services om te voorkomen dat aanvallers cloud- en firewallbeveiligingsbeleid ontwijken”,* zegt Sergei Shevchenko, threat research manager van SophosLabs. *“Securityteams moeten ook bescherming bieden tegen aanvallen van meerdere platforms. Tot nu toe waren Windows-gebaseerde middelen een typisch doelwit, maar aanvallers overwegen Linux vaker omdat clouddiensten populaire jachtgebieden zijn geworden. Het is een kwestie van tijd voordat meer cybercriminelen deze technieken overnemen.”*

**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](mailto:sandra@square-egg.be), GSM 0497 251816.