**Persbericht**

**SophosLabs waarschuwt voor 2017:**

**“Meer ransomware en meer dreigingen rondom Internet of Things”**

Brussel, 16 februari 2017 – **In aanloop naar de RSA Conference 2017 komt Sophos met de malware-voorspellingen voor de komende periode. Normaal gesproken ligt de focus van onze onderzoeksrapporten op Windows. Echter in dit rapport richt Sophos zich op de toenemende malwaredreigingen waar de risico's nooit altijd zo goed begrepen worden. Denk daarbij aan Linux, MacOs en Android-toestellen.**

SophosLabs heeft vier trends geïdentificeerd die in 2016 al aan het licht kwamen maar ook in 2017 een uitdaging blijven.

**Linux-malware op toestellen voor Internet of Things (IoT)**

Het rapport van Sophos begint met de toename van het gebruik van Linux bij het infecteren van IoT-toestellen. Dat kan van alles zijn: webcams en andere huishoudelijke apparatuur die op het internet zijn aangesloten. Standaardwachtwoorden, oude Linux-versies en gebrek aan encryptie kunnen deze apparatuur gevoelig maken.

**De aanwezigheid van Android-malware**

Daarnaast kijkt het rapport naar de top-10 malwarefamilies die Andriod-toestellen aanvallen. De meest prominente daarbij is Andr/PornClk: meer dan 20% van de door SophosLabs geanalyseerde gevallen in 2016 zijn van deze familie afkomstig. Het genereert geld door advertentie en lidmaatschapregistraties. Het downloadt Android Application Packages, creëert shortcuts op je scherm en verzamelt informatie zoals het ID van je toestel, je telefoonnummer en ander gevoelige informatie.

Het rapport kijkt ook naar ransomware zoals Andr/Ransom-I, die zich voordoet als een update voor je besturingssysteem en applicaties als Adobe Flash en Adult Player. Eenmaal gedownload, wordt het toestel ontvoerd. Ook al is deze malware nog niet zo wijd verspreid als andere malware (slechts goed voor 1% en komt niet voor in de top-10), toch is het wel belangrijk deze te noemen. De malware richt zich namelijk op toestellen met Android 4.3, de versie die nog steeds voor 10% van de Android-eigenaren wordt gebruikt en goed is voor 140 miljoen gebruikers wereldwijd.

**MacOS malware verspreidt ongewilde applicaties (PUA)**

Het rapport kijkt ook naar MacOS-malware die is ontworpen om codes te installeren die wachtwoorden ontvreemden, waaronder ransomware als OSX/KeRanger-A en verschillende kwaadwillende adware. Ook al heeft dit besturingssysteem minder infecties dan Windows, toch heeft MacOS er meer bij gekregen in 2016 waarbij verwacht wordt dat deze lijn zich voortzet.

**Microsoft Word Intruder-malware gaat verder dan Office**

Als laatste kijkt het rapport ook naar Windows-gebaseerde malware die voorheen alleen Word op de radar had maar nu hun grenzen verleggen en ook Flash aanvallen.

Voor het volledige Sophos-rapport:

<https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2017-malware-forecast-report.pdf?la=en>

**Connect with Sophos**

[Twitter](http://soph.so/CfuKd)

[LinkedIn](http://soph.so/Cfv36)

[Facebook](http://soph.so/CfvaA)

[Google+](https://plus.google.com/%2Bsophos)

[Spiceworks](http://soph.so/Cgbwa%20)

[YouTube](http://www.youtube.com/user/sophoslabs)

[Sophos Blog](http://blogs.sophos.com/)

[Naked Security News](http://nakedsecurity.sophos.com/)

**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, interviewmogelijkheden of beeldmateriaal:**

Square Egg, Sandra Van Hauwaert, Sandra@square-egg.be, 0032 497 251816