**Persbericht**

**“Android nog altijd doelwit van cybercriminelen”**

Brussel, 10 april 2017 – **Een recentelijk onderzoek van SophosLabs heeft uitgewezen dat Potentially Unwanted Applications-malware (PUA’s) voor Windows, Mac en Android zich vooral op Android-toestellen richt.**

De resultaten van het onderzoek geven tevens aan dat de cybercriminelen PUA’s, (programma’s die bijvoorbeeld adware bevatten en ongewenst toolbars installeren) misbruiken om voorbij beveiligingssystemen te glippen en zo toegang tot de Android- en Mac-apparatuur verkrijgen. Windows blijft nog steeds het besturingssysteem waarop criminelen zich richten, maar de ‘grimmigheid’ jegens Android is evident.

“*Hoe opener het systeem, des te gevoeliger het is voor malware*”, stelt Lars Putteneers, Security Advisor bij Sophos. “*Malware-schrijvers zien PUA’s als een perfecte manier om securitysystemen te omzeilen en hetzelfde doel te bereiken als met andere malware: geld verdienen*.”

**Cijfers liegen nooit**

De cijfers die door SophosLabs in 2016 zijn geanalyseerd geven het volgende weer:

* *Van alles wat Windows heeft aangevallen, waren 6% PUA’s terwijl 95% ‘straight up malware’ was;*
* *Van alles wat Android heeft aangevallen, was 74% pure malware en was 25% PUA’s;*
* *Tenslotte Mac: daar was malware goed voor 6% en PUA’s voor 94%.*

**Android-malware nader bestudeerd**

In Sophos’ *malware forecast* die eerder dit jaar verscheen, ontdekten onderzoekers malware die speciaal voor Android-toestellen is ontworpen. Hierbij werden in 2016 meer dan 8.500.000 verdachte Android-applicaties verwerkt. Meer dan de helft was óf malware óf PUA’s (waaronder ook adware). Van de grootste tien malware-families die zich op Android richtten, is Andr/PornClk de grootste (20%).

**Hoe te bestrijden?**

Ook al blijft Android-beveiliging een heet hangijzer, toch zijn er genoeg maatregelen die je kunt ondernemen om je te beveiligen:

* Gebruik Google Play
* Overweeg een Android anti-virusoplossing
* Vermijd apps met een slechte reputatie
* Patch vroegtijdig en patch zo vaak mogelijk

Voor Mac wordt aangeraden een real-time anti-virusoplossing te gebruiken of de security-oplossing van Apple zelf.

Eenzelfde advies geldt voor malware en PUA’s die zich op Windows richten. Patchen is een voorwaarde maar wees voorzichtig met (het openen van) bijlagen en links die via Outlook binnenkomen.

**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, GSM 0497 251816.