Beste,

Of het nu gaat om online spelprogramma’s, mobiele apps of wearable tech, feit is dat de technologie vandaag deel uitmaakt van alle aspecten van ons dagelijks leven. Deze hyperverbonden wereld heeft helaas een aantal nadelen, onder meer dat we allen, zonder uitzondering, extreem gevoelig zijn voor cyberaanvallen.

Dit jaar heeft het [Malware Report](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf?la=en) van Sophos aangetoond in welke mate malware in de dagelijkse technologie is binnengedrongen en hoe cybercriminelen almaar slimmer worden. Het is meer dan ooit van essentieel belang om de gebruikers attent te maken op de gevaren die op de loer liggen.

Veel mensen zijn ervan overtuigd dat ze nooit ofte nimmer het slachtoffer zullen zijn van een dergelijke aanval. Volgens het Amlo-onderzoek van Sophos hebben ze het bij het verkeerde eind. Sophos somt de belangrijkste risico’s van 2017 op, alsook de dreigingen in 2018.

* De omvang van de aanvallen met ransomware in 2017
* Hoe online gamen de niets vermoedende gebruiker aanvalt
* Het aantal apps met malware dat dit jaar op Android werd aangetroffen
* Overwegingen en prognoses voor 2018

Maak gerust gebruik van onderstaande informatie en neem contact met ons op voor een gesprek met een van de veiligheidsspecialisten van Sophos over de gevaren van cybercriminaliteit waaraan we dit jaar zijn blootgesteld, en over de prognoses voor volgend jaar.

Alvast bedankt,
Sandra Van Hauwaert

**Sophos 2017: de malware-tendensen en prognoses**

1. **Ransomware op elk platform –geen enkele draagbare computer of tablet die er nog aan ontsnapt!**

Dit jaar zorgde WannaCry wereldwijd voor veel opschudding met een cyberaanval die, volgens het laatste Malware Report van Sophos goed was voor meer den 45% van alle gedetecteerde ransomware, op de voet gevolgd door Cerber met 44.2% van de ransomware.

In september alleen al, bleek 30.4 percent van de malware op Android die door SophosLabs werd onderzocht ransomware te zijn. Volgens Sophos zou dit oplopen tot 45 percent in oktober. De meeste aanvallen treffen Windows-gebruikers, maar het aantal aanvallen op andere platformen blijft stijgen. Android, Mac en Linux zijn even goed het mikpunt geworden van cyberattacks.

De aanvallen met ransomware hebben de twee laatste jaren een nieuw doelwit. Nu treffen ze sectoren die meer belang hebben om te betalen, zoals instellingen uit de gezondheidssector, overheidsdiensten, vitale infrastructuren en kleine ondernemingen. Aangezien de aanvallen op ondernemingen uit de gezondheidssector bijzonder rendabel leken in termen van losgeld betalen of van verkoop van medische dossiers, was deze sector het geliefkoosde doelwit van 2017. Deze tendens zal zich ongetwijfeld in 2018 verder zetten.

1. **Malware verborgen in Android-apps**

Naar aanleiding van een onderzoek van Google Play kon Sophos vaststellen dat het aantal verschillende dreigingen het afgelopen jaar verdubbeld was. Een van de types malware, ‘GhostClicker’genaamd, was bijna een heel jaar lang in Google Play binnen geslopen als onderdeel van de bibliotheek-service. Hij vroeg toestemming voor *device administration* en simuleerde actief klik-advertenties waarmee geld kan worden verdiend.

Een andere, ergere dreiging was de ‘Lipizzan spyware’ die tot 100 toestellen kan besmetten. Dit aantal lijkt op het eerste gezicht mee te vallen, ware het niet dat het hier gaat om een precisiemalware die heel gericht tot doel heeft de telefonie te controleren en gegevens te ontfutselen van populaire apps en van e-mails, SMS, lokalisaties, telefoonoproepen en media.

Dit type malware zal niet verdwijnen en ook niet verminderen, integendeel. De cybercriminelen weten immers dat het werkt. Sophos geeft dan ook volgende adviezen aan gebruikers om hen te hoeden tegen Android-malware:

* Beperk je tot Google Play – ook al is het niet perfect, het doet bijzonder veel moeite om malware te voorkomen;
* vermijd apps die geen goede naam hebben;
* wees extra voorzichtig met de telefoon van het werk;
* verbeter snel en veel – ga na hoe de leverancier hierover denkt.
1. **Online gamen wordt gebruikt om ransomware en malware te verspreiden**

Bij online gamen werden dit jaar valse kopieën van het populaire spel ‘King of Glory’ gebruikt om ransomware te verspreiden. Het waarschuwingsscherm dat hierbij werd gebruikt leek op dat van WannaCry en vroeg particuliere gebruikers om het losgeld te betalen via Wechat, Alipay en QQ, drie betaalsystemen die in China gebaseerd zijn.

De afgelopen vier jaar is het aantal malware apps almaar gestegen. In 2017 zelfs tot bij de 3.5 miljoen. Deze tendens zal zich in 2018 verder zetten met nog betere en nog meer misleidende valstrikken in de online games.

1. **Het einde van de data-breaches is niet in zicht**

Het grote nadeel van deze hyperverbonden wereld is dat mensen vandaag extreem kwetsbaar zijn voor cyberaanvallen, zoals we nog onlangs hebben kunnen zien met de [Uber Hack](https://nakedsecurity.sophos.com/2017/11/22/uber-suffered-massive-data-breach-then-paid-hackers-to-keep-quiet/), waarvan niet minder dan 2.7 miljoen chauffeurs en piloten het slachtoffer waren. En er is weinig kans dat het hacken van gegevens in 2018 zal verminderen. Met de invoering van de GDPR-wet in mei volgend jaar, zal dit meer dan ooit een hot item zijn.

1. **2018 en daarna**

Niemand weet wat er in 2018 zal gebeuren, maar we kunnen ervan uitgaan dat Android en Windows de belangrijkste doelwitten zullen blijven voor ransomware en andere malware. Het e-mailverkeer blijft de geliefkoosde aanvalsvector en belangrijkste dreiging voor bedrijven, zeker als het gaat om een gerichte aanval.

Dit zijn de vier tendensen van 2017, die zich naar alle waarschijnlijkheid in 2018 zullen voortzetten:

1. een opstoot van ransomware aangedreven door RaaS en versterkt door de heropleving van *worms*;
2. een explosie van malware Android op Google Play en andere websites en apps;
3. nog meer inspanningen om Macs te besmetten; en
4. aanhoudende dreigingen voor Windows, die nog worden aangesterkt door de doe-het-zelf exploitatiepakketten die de aanvallen op de gevoelige plekken van Microsoft Office vergemakkelijken.