Bonjour,

La technologie fait aujourd’hui partie de notre quotidien, que ce soit via des jeux en ligne et des applications portables qu’avec des vêtements intelligents. Une société hyperconnectée comme la nôtre nous rend hélas tous, autant que nous sommes, extrêmement vulnérables aux cyberattaques.

Cette année, le [Malware Report](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf?la=en) de Sophos a démontré comment les maliciels se sont insinués dans la technologie quotidienne et comment les cybercriminels sont chaque jour de plus en plus malins. Il est plus que jamais important d’informer les consommateurs des dangers qui les guettent.

Alors que de nombreux consommateurs sont convaincus qu’ils ne seront jamais victime d’une telle attaque, l’étude Amlo de Sophos vient de démontrer le contraire. Sophos énumère les risques majeurs de 2017, ainsi que ceux qui nous menacent en 2018.

* L’étendue des attaques de ransomware de 2017
* Comment les jeux en ligne prennent les consommateurs par inadvertance
* Le taux d’applications malveillantes Android détectées cette année
* Considérations et prévisions pour 2018

Surtout, n’hésitez pas à faire usage des informations ci-dessous. Faites-nous savoir si vous aimeriez avoir un entretien avec un des experts de la sécurité chez Sophos au sujet des dangers de cybercriminalité qui menacent les consommateurs cette année, ainsi qu’au sujet des prévisions de l’année prochaine.

Merci,
Sandra Van Hauwaert

**Sophos 2017 les tendances et prédictions de Malware**

1. **Du ransomware sur chaque plateforme –ni vos portables ni vos tablettes n’y échappent**

Cette année, WannaCry a secoué le monde avec une cyberattaque représentant plus de 45% de tous les ransomwares détectés, suivie de Cerber représentant 44.2%, conformément au dernier Malware Report de Sophos.

Rien qu’en septembre déjà, 30.4 pour cent des logiciels malveillants sur Android traités par SophosLabs se sont avérés être du ransomware. Selon Sophos, il devrait atteindre près de 45 pour cent en octobre. La majorité de ces attaques visent des utilisateurs de Windows, mais le nombre d’attaques sur d’autres plateformes ne cesse d’augmenter. Android, Mac et Linux sont également concernés.

Les attaques de ransomware ont changé de cible les deux dernières années et visent aujourd’hui des entreprises qui ont davantage intérêt à payer, telles les organismes du secteur des soins de santé, les autorités publiques, les infrastructures essentielles et les petites entreprises. Comme les attaques ciblées sur les soins de santé se sont avérées les plus lucratives en termes de paiement de la rançon ou de vente de dossiers médicaux, ce secteur a été la cible privilégiée en 2017 et tout porte à croire que cette tendance se poursuivra en 2018.

1. **Le malware dissimulé dans les applications Android**

En examinant Google Play, Sophos a constaté que le nombre de menaces différentes avait doublé depuis l’année dernière. L’un des types de malware, dénommé ‘GhostClicker’, s’était faufilé dans Google Play durant près d’une année, dissimulé comme une partie du service librairie. Il demandait une autorisation de *device administration* et simulait les publicités à cliquer génératrices de recettes.

Autre triste constatation, le spyware Lipizzan infectait jusqu’à 100 appareils. Si cela semble relativement peu à première vue, il s’agissait en fait d’un logiciel malveillant de précision ciblé, destiné à surveiller les activités téléphoniques et à soutirer des données d’applications populaires, y compris les e-mails, SMS, localisations, appels vocaux et médias.

Ce type de malware ne va pas disparaître ni diminuer, loin de là, car les cybercriminels savent que ça marche. Dès lors, pour éviter d’être victime de malware Android, Sophos conseille ce qui suit aux consommateurs :

* Limitez-vous à Google Play – même s’il n’est pas parfait, il s’efforce au moins de prévenir l’arrivée de malware ;
* Evitez les applications qui n’ont pas bonne réputation ;
* Soyez d’autant plus vigilants lorsque vous utilisez le téléphone du bureau ;
* Corrigez vite et souvent – Contrôlez l’attitude des fournisseurs en la matière.
1. **Les jeux en ligne sont utilisés pour propager le ransomware et du malware**

Pour ce qui est des jeux en ligne, de fausses copies du jeu populaire ‘King of Glory’ ont été utilisées cette année pour propager du ransomware. L’écran d’avertissement utilisé imitait celui de l’épidémie WannaCry et invitait les particuliers à payer la rançon en utilisant les modes de paiement Wechat, Alipay et QQ basés en Chine.

Le nombre d’applications malveillantes a constamment augmenté ces quatre dernières années, jusqu’à atteindre près de 3.5 millions en 2017. Cette tendance se poursuivra en 2018, avec des pièges encore plus trompeurs cachés dans les jeux en ligne.

1. **Les fuites de données ne sont pas prêtes de disparaître**

Notre société hyperconnectée a pour inconvénient majeur que les gens sont extrêmement vulnérables aux cyberattaques, comme nous avons pu le voir les dernières semaines avec l’[Uber Hack](https://nakedsecurity.sophos.com/2017/11/22/uber-suffered-massive-data-breach-then-paid-hackers-to-keep-quiet/), qui a affecté quelque 2.7 millions de conducteurs et pilotes. Nous ne pensons pas que le piratage de données diminuera en 2018, loin de là. Avec l’entrée en vigueur de la loi GDPR en mai prochain, les sujets restera d’actualité et sera plus brûlant que jamais.

1. **2018 et plus tard**

S’il est impossible de prédire ce qui se passera en 2018, il est un fait qu’Android et Windows demeureront les principales cibles de ransomware et d’autres logiciels malveillants. L’e-mail sera aussi le premier vecteur d’attaque menaçant la cyber sécurité des entreprises, spécialement en cas d’attaque ciblée.

Les quatre tendances enregistrées en 2017 qui domineront probablement en 2018, sont :

1. une poussée de ransomware alimentée par RaaS et amplifiée par le retour en force de vers informatiques ;
2. une explosion de malware Android sur Google Play et ailleurs ;
3. des efforts accrus pour infecter les ordinateurs Mac ; et
4. des menaces persistantes pour Windows, alimentées par des packages d’exploitation à installer soi-même qui facilitent les attaques contre les vulnérabilités de Microsoft Office.