COMMUNIQUÉ DE PRESSE

La technologie Kaspersky Lab détecte un deuxième exploit du jour zéro consécutif pour Microsoft Windows en seulement un mois

Utrecht, le 14 novembre 2018 – En octobre 2018, la technologie Automatic Exploit Prevention de Kaspersky Lab, intégrée à la plupart des produits de l'entreprise, a détecté un nouvel exploit pour une vulnérabilité du jour zéro dans Microsoft Windows. Il s'agissait du deuxième exploit du jour zéro consécutif utilisé dans une série de cyberattaques au Moyen-Orient en un mois seulement. Après avoir été signalée par Kaspersky Lab, la vulnérabilité a été corrigée par Microsoft le 13 novembre.

Les attaques qui passent par des vulnérabilités du jour zéro sont parmi les plus dangereuses, car elles impliquent l'exploitation d'une faiblesse non découverte et non réparée, autrement dit, elles sont difficiles à détecter et à prévenir. Si elle est découverte par des criminels, une telle vulnérabilité pourrait être utilisée pour la création d'un exploit, à savoir un programme malveillant spécial qui ouvrira l'accès à un système entier. Ce scénario d'attaque de « menace cachée » est largement exploité par des acteurs sophistiqués dans les attaques APT (menaces persistantes avancées).

L'analyse de Kaspersky Lab sur le nouvel exploit a conduit les experts à une vulnérabilité du jour zéro inconnue à ce jour. Bien que la méthode d'introduction soit encore inconnue, l'exploit a été exécuté par la première étape d'un installateur de programme malveillant afin d'obtenir les privilèges nécessaires à la persistance sur le système de la victime. L'exploit a permis de ne cibler que la version 32 bits de Windows 7.

Selon les experts de Kaspersky Lab, l'identité de l'acteur responsable de ces attaques reste un mystère, mais l'exploit développé est utilisé par au moins un ou plusieurs acteurs APT. Pour plus de détails, veuillez contacter intelreports@kaspersky.com.

Dès le moment de sa découverte, les experts de Kaspersky Lab ont immédiatement signalé la vulnérabilité à Microsoft.

Quelques semaines auparavant, au début du mois d'octobre, un autre exploit pour une vulnérabilité du jour zéro avait été détecté dans Microsoft Windows. Il était transmis aux victimes via une porte dérobée en PowerShell. La technologie de Kaspersky Lab a identifié la menace de manière proactive et l'a également notifiée à Microsoft.

« L'automne 2018 est devenu une saison assez « chaude » pour ce qui est des vulnérabilités du jour zéro. En un mois seulement, nous en avons découvert deux de ce type et avons détecté deux séries d'attaques dans une région. La discrétion des activités des acteurs de la cybermenace nous rappelle qu'il est d'une importance cruciale pour les entreprises de disposer de tous les outils et solutions nécessaires qui seraient suffisamment intelligents pour les protéger de menaces aussi sophistiquées. Sinon, elles pourraient faire l'objet d'attaques ciblées complexes qui surgiront de nulle part », a constaté Anton Ivanov, expert en sécurité chez Kaspersky Lab.

Pour éviter les exploits du jour zéro, Kaspersky Lab recommande de mettre en œuvre les mesures techniques suivantes :

- si possible, évitez d'utiliser des logiciels dont la vulnérabilité est connue ou qui ont été récemment utilisés dans des cyberattaques ;
- assurez-vous que le logiciel utilisé dans votre entreprise est régulièrement mis à jour avec les versions les plus récentes. Les produits de sécurité dotés de capacités d'évaluation de la vulnérabilité et de gestion des correctifs peuvent aider à automatiser ces processus ;
- utilisez une solution de sécurité robuste telle que Kaspersky Endpoint Security for Business qui est équipée de capacités de détection basées sur le comportement pour assurer une protection efficace contre les menaces connues et inconnues, y compris les exploits ;
- si votre entreprise peut faire l'objet d'attaques ciblées, utilisez des outils de sécurité avancés comme Kaspersky Anti Targeted Attack Platform (KATA) ;
- donnez à votre équipe de sécurité l'accès à la source des renseignements les plus récents sur la cybermenace.

Pour en savoir plus, surfez sur Securelist.com.

À propos de Kaspersky Lab

Présente sur le marché depuis plus de 20 ans, Kaspersky Lab est une société de cybersécurité opérant dans le monde entier. L'expertise et l'expérience approfondies de Kaspersky Lab se traduisent constamment en solutions et services de sécurité pour protéger les entreprises, les infrastructures critiques, les pouvoirs publics et les particuliers. Le portefeuille étendu de solutions de protection et de sécurité de la société comprend la référence en matière de protection de terminaux et de solutions et services de sécurité spécialisés pour lutter contre les menaces numériques avancées et en évolution continue. Les technologies de Kaspersky Lab offrent une protection à plus de 400 millions d'utilisateurs et l'entreprise aide 270 000 clients professionnels à protéger leurs biens les plus précieux. Plus d'informations sur www.kaspersky.com.

Note pour les rédactions:

Le 13 novembre, Kaspersky Lab organise en ligne une table ronde en direct sur la restauration de la confiance dans la cyber-sécurité et la réduction au minimum des risques, entraînées par la transparence. D'éminents experts du monde de la sécurité informatique prendront part à cette table ronde. Le débat sera diffusé depuis Zurich et il fait partie intégrante du Kaspersky Transparency Summit organisé dans cette ville. De plus amples détails et des informations sur l'inscription sont disponibles ici.

Contacts :

Kaspersky Lab
Caroline Breure
Tél. : +31 (0)30 – 752 95 00
caroline.breure@kaspersky.nl

The Communication Force
Jan Poté
Tél. : +32 (0) 475 925 582
jan.pote@gmail.com