Kaspersky Lab descubre una vulnerabilidad zero-day de Windows utilizada por un actor de amenazas identificado recientemente

---

Las tecnologías automatizadas de Kaspersky Lab han detectado una nueva vulnerabilidad en Microsoft Windows. Parece que al menos dos actores de amenazas han utilizado esta vulnerabilidad, entre ellos el recientemente descubierto SandCat. Este es el cuarto exploit zero-day que se descubre gracias a la tecnología Automatic Exploit Prevention de Kaspersky Lab. Kaspersky Lab informó de la vulnerabilidad - CVE-2019-0797- a Microsoft, que ya ha lanzado un parche.

Las vulnerabilidades de día-cero son errores de software desconocidos hasta ese momento que los cibercriminales pueden aprovechar para introducirse en la red y en los dispositivos de las víctimas. El nuevo exploit usa una vulnerabilidad en el subsistema gráfico de Microsoft Windows para lograr una escalada de privilegios locales, lo que otorga al ciberdelincuente un control total sobre el ordenador de la víctima. La muestra de malware analizada revela que el exploit se dirige contra las versiones del sistema operativo Windows que abarcan desde Windows 8 a Windows 10.

Los analistas creen que el exploit detectado podría haberse utilizado por varios actores de amenazas, incluyendo -aunque no limitándose- FruityArmor y SandCat. FruityArmor es conocido por haber utilizado anteriormente Zero-days; mientras que SandCat es un nuevo actor de amenazas recientemente identificado.

"El descubrimiento de una nueva vulnerabilidad Zero-day de Windows, explotada muy activamente, muestra que esas herramientas siguen siendo de gran interés para los actores de amenazas y las organizaciones necesitan soluciones de seguridad que protejan contra ese tipo de amenazas desconocidas. También reafirma la importancia de la colaboración entre la industria de la seguridad y los desarrolladores de software: la búsqueda de errores, la divulgación responsable y la aplicación rápida de parches, son las mejores maneras de mantener a los usuarios a salvo de amenazas nuevas y emergentes", dijo Anton Ivanov, experto de seguridad de Kaspersky Lab.

La vulnerabilidad explotada fue detectada por la tecnología automática de prevención de exploits de Kaspersky Lab, incluida en la mayoría de los productos de la compañía.

Los productos de Kaspersky Lab detectan exploits como:

- HEUR:Exploit.Win32.Generic
- HEUR:Trojan.Win32.Generic
- PDM:Exploit.Win32.Generic

Kaspersky Lab recomienda tomar las siguientes medidas de seguridad:

- Instalar, tan pronto como sea posible, el parche de Microsoft para la nueva vulnerabilidad.

- Actualizar, de forma regular, todo el software utilizado en su organización, sobre todo cada vez que se lance un nuevo parche de seguridad. Los productos de seguridad con capacidades de análisis de vulnerabilidades y gestión de parches pueden ayudar a automatizar estos procesos.

- Instalar una solución de seguridad probada, como Kaspersky Endpoint Security, que esté dotada con capacidades de detección basadas en el comportamiento para una protección efectiva contra amenazas conocidas y desconocidas, incluidas las vulnerabilidades.

- Utilizar herramientas de seguridad avanzadas como Kaspersky Anti Targeted Attack Platform (KATA) si su empresa requiere de una protección altamente sofisticada.

- Garantizar el acceso del equipo de seguridad de la organización a la información de ciberamenazas más reciente. Los informes privados sobre los últimos desarrollos en el panorama de amenazas están disponibles para los clientes de Kaspersky Intelligence Reporting. Para más detalles, contactar con intelreports@kaspersky.com.

- Por último, pero no menos importante, asegurarse de que el personal de la organización está formado en los aspectos básicos de la higiene de la ciberseguridad.

Para más detalle sobre la nueva amenaza, lea el informe en Securelist.

Para descubrir más sobre las tecnologías que detectaron este y otros zero-days en Microsoft Windows, Kaspersky Lab pone a su disposición este webinar grabado.

Sobre Kaspersky Lab

Kaspersky Lab es una empresa global de ciberseguridad con más de 20 años de trayectoria en el mercado. El profundo conocimiento de Kaspersky Lab en inteligencia de amenazas y seguridad se traduce en el desarrollo de soluciones de seguridad y servicios de última generación para proteger a empresas, infraestructuras críticas, gobiernos y consumidores de todo el mundo. El extenso portfolio de seguridad de la compañía incluye su reputada solución de protección de endpoints junto soluciones y servicios de seguridad especializados para combatir sofisticadas amenazas digitales en constante evolución. Más de 400 millones de usuarios están protegidos por las tecnologías de Kaspersky Lab y ayudamos a 270.000 clientes corporativos a proteger lo que más les importa. Más información en www.kaspersky.es

Síguenos en:

http://twitter.com/#!/KasperskyES

http://www.youtube.com/user/kasperskyespana

http://www.facebook.com/kasperskyes

http://blog.kaspersky.es/

Para más información, contactar con:

eVerything PR
Virginia Frutos
Tel. +34 91 551 98 91
Mov: 670 502 902
Email: virginia.frutos@everythinkpr.com

Kaspersky Lab Iberia
Vanessa González
Directora de Comunicación
Tel. +34 91 398 37 52
Email: vanessa.gonzalez@kaspersky.es