Masterhacks – Aunque muchos usuarios de Mac están seguros de que no sufrirán por malware, FruitFly es la prueba de que no es así.

Investigadores encontraron una pieza inusual de malware, que ha infectado computadoras Mac por algunos años.

FruitFly funciona en segundo plano, espiando a los usuarios por medio de la cámara web de la computadora, captura imágenes de lo que ocurre en la pantalla y registra puntos clave.

Malwarebytes descubrió la primera cepa a inicios de 2017, pero recientemente apareció una segunda versión llamada FruitFly 2.

El investigador jefe de seguridad de Synack, Patrick Wardle, encontró 400 computadoras infectadas con la nueva cepa, y afirma que es probable que existan muchos más casos.

No se sabe exactamente cuanto tiempo ha estado infectado computadoras este malware, pero los investigadores encontraron ediciones del código para trabajar en Mac, específicamente Yosemite, que fue lanzado en octubre de 2014, lo que deja pensar que el malware surgió antes de ese año.

Tampoco se sabe quién está detrás del malware, Thomas Reed, de Malwarebytes llamó a la primera versión como *«diferente de todo lo que he visto antes».*

Wardle afirma que existen múltiples versiones de FruitFly. El software malicioso tiene las mismas técnicas de espionaje, pero el código es diferente en cada versión.

Luego de meses de análisis de la nueva cepa, Wardle descifró partes del código y configuró un servidor para calcular el tráfico de computadoras infectadas.

«Inmediatamente, toneladas de víctimas que habían sido infectadas con este malware empezaron a conectarse conmigo», afirmó Wardle, y añadió que podría ver cerca de 400 nombres de equipos infectados, así como direcciones IP.

> *«Los usuarios de Mac tienen más confianza», dice Wardle, «Podríamos no ser tan cuidadosos como deberíamos estar en Internet o abrir archivos adjuntos en un correo electrónico».*

Un informe de McAfee afirma que el malware que afecta a las Mac se disparó en 2016, pero la mayoría era adware, virus de publicidad.

El FBI no confirma ni niega la existencia de investigaciones al respecto, y Apple por otro lado, no ha dado comentarios.

Wardle es exanalista de la NSA, y descartó la posibilidad de que un hacker que trabaje para el gobierno sea responsable. *«Creo que sus objetivos eran mucho más insidiosos y enfermos: espiar a la gente»,* asegura.