Vulnerabilidad Superfish Ha Sido Encontrada En Diversas Aplicaciones

Vulnerabilidad Superfish Ha Sido Encontrada En Diversas Aplicaciones

Recientemente se ha encontrado preinstalado software de publicidad en computadoras portátiles de Lenovo, el cual ha sido llamado como Superfish. Facebook ha descubierto al menos 12 juegos más usando la misma tecnología HTTPS, que dio la capacidad al malware Superfish para evadir el proceso de certificado.

La **vulnerabilidad Superfish** afectó a decenas de computadoras portátiles de Lenovo vendidas antes de enero de 2015, expone a los usuarios a una técnica de robo para interceptar y descifrar las conexiones HTTPS, la manipulación de las páginas y la **inyección de anuncios publicitarios**.

Hijacking SSL

Superfish utiliza una técnica conocida como «Hijacking SSL«, parece ser un Framework adquirido a una tercera empresa, ***Komodia***, de acuerdo con un blog escrito por **Matt Richard**, un investigador de amenazas en el equipo de seguridad de Facebook. La técnica tiene capacidad de eludir las protecciones de Secure Sockets Layer (SSL), mediante la modificación de la pila de red de los equipos que ejecutan su código subyacente.

Komodia instala un certificado de CA raíz autofirmado, el cual

permite a la biblioteca **interceptar y descifrar las conexiones encriptadas** desde cualquier sitio web HTTPS protegida en Internet.

Uso Común De Biblioteca

El investigador también dice que Facebook descubrió más de una **docena de aplicaciones de software,**las cuales usan la biblioteca Komodia, esta cuenta con la misma funcion de Hijacking de Superfish:

- CartCrunch Israel LTD
- WiredTools LTD
- Say Media Group LTD
- Over the Rainbow
- Tech System Alerts
- ArcadeGiant
- Objectify Media Inc
- Catalytix Web Services
- OptimizerMonitor

> *«Lo que todas estas aplicaciones tienen en común, es que hacen que la gente sea menos segura a través del uso de un CA raíz fácilmente obtenido, proporcionan poca información sobre los riesgos de la tecnología, y en algunos casos son difíciles de eliminar, » según comentó Richard.*

Biblioteca Komodia, Fácil De Detectar

En 2012, el gigante de las Redes Sociales inició un proyecto con investigadores de la Universidad Carnegie Mellon, con el fin de medir qué tan sensible es el SSL a un ataque man-in-the-middle (MitM).

Los investigadores dijeron que la biblioteca Komodia se puede

detectar fácilmente como el software que instala la CA raíz, y esta contiene una serie de atributos fácilmente investigables que permiten al equipo coincidir con los certificados que ven en la naturaleza con el software actual.

Como Identificar Superfish

Richard también publicó los hashes criptográficos SHA1, que se utilizaron en la investigación para identificar el software que contiene las bibliotecas de código Komodia. La lista de hashes SHA1 son:

- 0cf1ed0e88761ddb001495cd2316e7388a5e396e
- 473d991245716230f7c45aec8ce8583eab89900b
- fe2824a41dc206078754cc3f8b51904b27e7f725
- 70a56ae19cc61dd0a9f8951490db37f68c71ad66
- ede269e495845b824738b21e97e34ed8552b838e
- b8b6fc2b942190422c10c0255218e017f039a166
- 42f98890f3d5171401004f2fd85267f6694200db
- 1ffebcb1b245c9a65402c382001413d373e657ad
- 0a9f994a54eaae64aba4dd391cb0efe4abcac227
- e89c586019e259a4796c26ff672e3fe5d56870da

El investigador llegó a invitar a los investigadores de seguridad informática a utilizar estos hashes con el fin de identificar el software potencialmente más peligroso que circula a través de Internet.