Mac OSX

Seguridad

Protege tu Mac frente amenazas con + seguridad

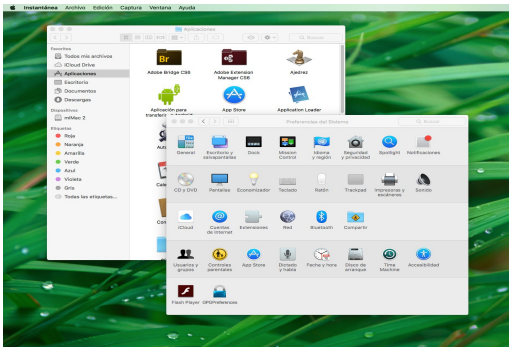
PROBLEMÁTICA ACTUAL DE LA SEGURIDAD EN EQUIPOS Mac OS X

José Luis Prado Seoane
IT Security Researcher
joseluispradoseoane.wordpress.com

La introducción con fuerza en el mercado de escritorio de otros sistemas operativos alternativos mas allá del conocido ®Windows como son todos aquellos basados en GNU-Linux; Ubuntu, Mint, SuSe, Fedora,.., y aquellos otros basados en Unix como el cada vez mas extendido Mac OSX, han transformado la oferta comercial en el ámbito del usuario final así como, extendido o amplificado las amenazas asociadas en lo que a Ciberseguridad se refiere.

La creencia existente de que todo tipo de amenazas relacionadas con Malware; *Virus clásicos, Gusanos de red, Troyanos, Spyware, Roothits, etc.-* , afectan únicamente a los sistemas basados en Windows es un error.

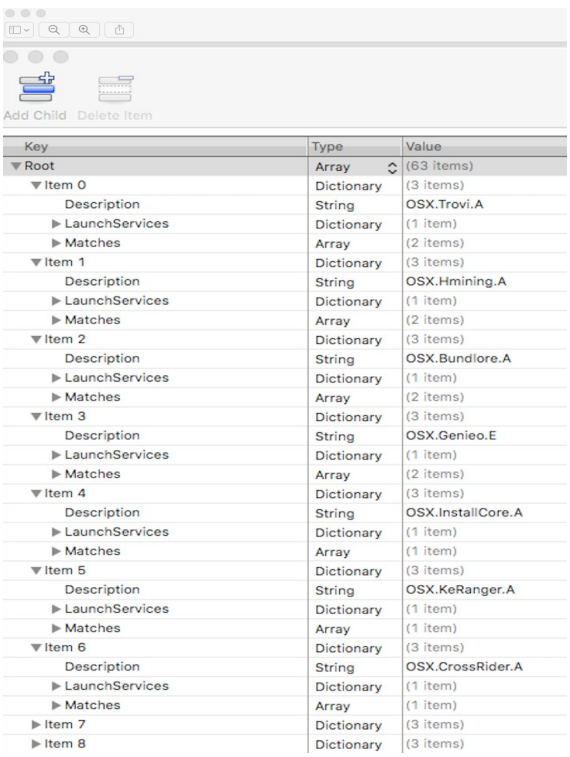
Tanto los sistemas basados en GNU-Linux o Mac OSX están expuestos a todo tipo de amenazas relacionadas con el Malware, que nadie lo dude, es una amenaza real y en algunos casos en concreto muy difíciles de detectar.



El creciente aumento de amenazas por Malware en entornos Mac OSX se debe principalmente a que tanto Hackers como Ciberdelincuentes han puesto su foco de atención en él por la gran aceptación que están teniendo en el mercado los productos de la firma ®Apple, no es más que pura estadística, cuantos más sistemas existen más aumentan las posibilidades de infección y compromiso, y ellos lo saben.

Todo ello ha llevado a la firma ®Apple a corregir errores, reforzar e implementar nuevas soluciones de seguridad internas en sus versiones recientes de OSX, que permitan proteger a los usuarios ante este tipo de amenazas. A grandes rasgos son las siguientes;

- Un Antivirus interno con una base de firmas estáticas de Malware conocido que permita detectar amenazas en base a un Hash.
- Software para análisis, comprobación y aislamiento sandbox, que ayuda a nuestro Mac a proteger los componentes críticos del sistema y todas aquellas aplicaciones (Apps) maliciosas descargadas desde Internet. OSX analiza y comprueba digitalmente (firmas) todas las descargas de software de su tienda de aplicaciones (App Store) y todas aquellas de origen desconocido, no olvidemos que a diferencia del sistema operativo IOS implementado en dispositivos IPHONE que si existen restricciones en la instalación de aplicaciones (Apps) en la que sólo se admiten aplicaciones firmadas digitalmente, en los sistemas OSX no existe tal restricción permitiendo estas descargas de orígenes desconocidos, dando la opción al usuario de poder configurar el nivel de seguridad que estime oportuno en las preferencias de su sistema.

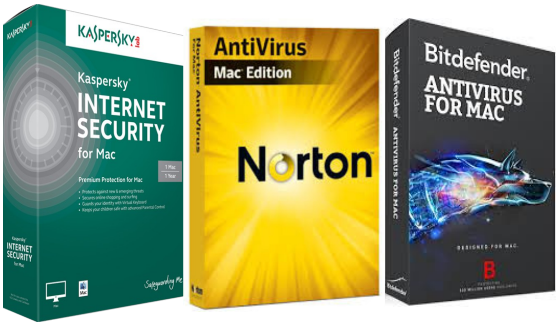


Mac OSX

Seguridad

Protege tu Mac frente amenazas con + seguridad

Además de las soluciones técnicas de seguridad proporcionadas por Apple en todos sus Mac OSX, todo usuario responsable también debería instalar y configurar un sistema Antivirus externo de la cantidad de opciones existentes en el mercado. Pero ya se sabe en la buena elección está la clave.



Hasta el momento he resumido la problemática existente en entornos OSX, soluciones de seguridad implementadas y reforzadas por el fabricante y las opcionales externamente además, aprovecho para recordar la importancia que tiene las actualizaciones periódicas (Updates) de nuestro sistema y aplicaciones que nos permitirá solucionar problemas o fallos de seguridad existentes, no olvide u omita esta característica, su seguridad está en juego.

El disponer de estas soluciones internas y externas de seguridad y de Updates periódicos, aumenta el grado de nuestra seguridad no cabe ninguna duda al respecto, pero como todo lo relacionado con la informática, nada es seguro cien por cien. El sistema Antivirus interno del OSX y en función de la versión existente es estático, lo que significa que puede presentar problemas ante la modificación u ofuscación del Malware, algo que los desarrolladores de códigos maliciosos lo saben, es uno de los motivos de porque existen en la actualidad tantos miles de detecciones de Malware a diario, pero que en la mayoría de los casos no dejan de ser “modificaciones de los mismos” que evitan en todo caso ser detectados por los sistemas Antivirus, y si la base de datos de firmas utilizada en base a un Hash inequívoco y estático no se actualiza de una forma periódica, hace muy difícil su detección.

Por no hablar de métodos de infección complejos que intentan saltarse el sistema de errores y de firma digital implementados así como, métodos de persistencia o Hooking para alterar o modificar el comportamiento del sistema operativo para comprometer la información, el objetivo de todo Hacker o Ciberdelincuente.

Nadie puede asegurar al cien por cien que su sistema Mac OS X está libre de algún tipo de Malware, y aunque las medidas existentes están ahí, nunca serán suficientes. Mi consejo y en función de que tipo de información manejemos en nuestro equipo, ya que no es lo mismo el uso que pueda hacer un particular, que una empresa o colectivo, aunque desde el punto de la protección de datos y la Privacidad todo es importante, es ponernos en manos de una empresa de Ciberseguridad o expertos especializados en estos sistemas, que permita realizar un examen más exhaustivo y preciso del mismo.

- Verificar nuestro equipo y realizar las actualizaciones del sistema operativo y aplicaciones existentes
- Instalación de herramientas de seguridad y gestión de opcionales del sistema; Instalación y configuración del Antivirus externo para la protección frente a Malware, antiphishing con protección de identidad y privacidad, gestión de orígenes, sistemas de cifrado de datos, Backups, cifrado en comunicaciones...
- Comprobación exhaustiva a nivel técnico de las aplicaciones instaladas en el equipo con independencia de todas aquellas instaladas a través de la tienda oficial de Apple (App Store) o de orígenes desconocidos.
- Detección de Rootkits y Backdoors, alteraciones en binarios,persistencias, comprobación de procesos,conexiones de red,fallos de configuración,verificación y corrección de permisos,análisis y protección dinámica de librerías..
- Formar al usuario en el uso correcto de su sistema e Internet; medidas de seguridad, análisis,Backups,como gestionar sus Updates, navegación Web segura, comunicaciones seguras ...