Mac y Linux Los Próximos Objetivos De Los Programas Maliciosos

El último informe mensual del especialista en seguridad de Internet Doctor Web, muestra que mientras los *usuarios de Windows y Android* no tienen una causa para sentirse seguros, noviembre vio un número importante de **programas maliciosos dirigidos a Mac OS X y Linux**.

Los troyanos siguen siendo la *forma más popular de ataque* que componen el **8.7 por ciento de todo el malware detectado**. Trojan.InstallCore.12, que instala diferentes programas publicitarios, barras de herramientas y extensiones del navegador, ocupa el primer lugar. El BackDoor.Andromeda.404, que descarga otros programas maliciosos en el sistema infectado, ocupa el segundo lugar.

En noviembre el BackDoor.Andromeda.404 fue distribuido en grandes cantidades por **correo electrónico usando una campaña masiva de spam**. Se representó el 2,4 por ciento del malware detectado por Doctor Web. La mayor parte de malware incluye una serie de *programas que buscan robar información confidencial*.

Varios de los nuevos ejemplos de **software malicioso para OS X**, se han añadido a la base de datos de Doctor Web. Estos incluyen Mac.BackDoor.Ventir.2, un backdoor que puede ejecutar comandos desde un servidor remoto, ingrese pulsaciones de teclas y transmitir información a los delincuentes. Particularmente Mac.BackDoor.WireLurker.1 es astuto, ya que espera el momento en que un dispositivo iOS está conectado a un Mac infectado y luego sube sus archivos en el dispositivo. Incluso viene en dos versiones, una ***destinada a los dispositivos con jailbreak***, mientras que el otro es para los

dispositivos iOS inalterados. Se aprovecha de la función de «aprovisionamiento de la empresa», que permite a las empresas para eludir la AppStore e instalar aplicaciones en los dispositivos de sus empleados.

Los **Sistemas Linux han sido blanco de Linux.BackDoor.Fgt.1,** el cual escanea direcciones IP aleatorias en internet y lanza un ataque de fuerza bruta en un intento de establecer una conexión Telnet con sus nodos. Si tiene éxito, los comandos de la máquina atacada descargan un script especial. Especialmente modifica los repositorios para instalar automáticamente programas maliciosos, pero tambien afecta otro tipos de dispositivos, como routers.

Android no escapa a las nuevas amenazas, siendo detectado un gran número de programas maliciosos. Muchos de estos son troyanos bancarios, destinados a robar dinero de cuentas de usuarios que acceden en dispositivos comprometidos. Por ejemplo, Android.BankBot.33.origin está dirigido a los usuarios de banca por Internet de Rusia. Emplea comandos SMS para transferir secretamente dinero a la cuenta de los intrusos y oculta las respuestas SMS desde el banco, para que el usuario no se entere de las transacciones no autorizadas. Además, se puede cargar una página web falsa en el navegador para atraer a los usuarios en la presentación de sus credenciales en línea.

Para obtener más información acerca de la última actividad de los virus y usar un escáner online gratuito para archivos maliciosos y enlaces, puedes visitar el sitio Doctor web.