PANDA
CLOUDINTERNETPROTECTION

Simply... Evolution

FALSOS ANTIVIRUS: UNA AMENAZA CRECIENTE

PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD EMAIL PROTECTION

PANDA CLOUD INTERNET PROTECTION

PANDA SECURITY

FALSOS ANTIVIRUS: UNA AMENAZA CRECIENTE

Google ha anunciado que las páginas pertenecientes a falsos antivirus representan el 60% del malware descubierto en dominios que incluyen términos de búsqueda populares. El equipo de investigación de Panda Security ha demostrado que las búsquedas de términos populares, como los mostrados en Google trends, pueden contener hasta un 90% de enlaces maliciosos que redirigen a páginas de falsos antivirus entre los primeros 100 resultados. Aún más alarmante resulta el hecho de que los atacantes son cada vez más expertos en situar enlaces maliciosos en los primeros lugares de los resultados de búsquedas populares.redes contra los ataques actuales.

A pesar de que la amenaza de los falsos antivirus está creciendo y representa más del 60% del malware proveniente de las búsquedas de Google, no se detecta bien. Google puede tardar varios días en eliminar algunos de los enlaces maliciosos. Cinco días después de un ataque, aún puede haber búsquedas populares que contengan enlaces maliciosos en las primeras 10 páginas de resultados. Además, como los atacantes se ocultan detrás de múltiples sitios legítimos y emplean nuevos dominios cada día para albergar las páginas de los falsos antivirus, las herramientas de diagnóstico como Google Safe Browsing no ofrecen una protección suficiente.

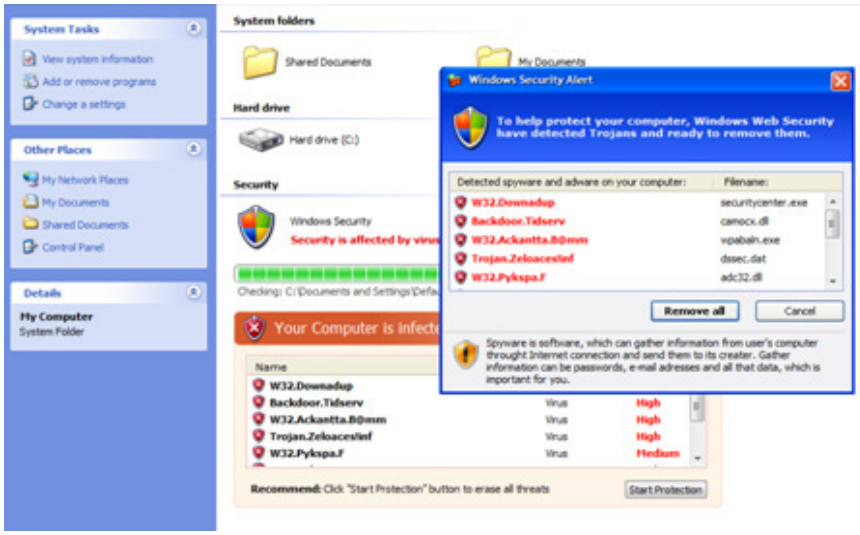


Imagen 1: Página de un falso antivirus

Mediante el empleo de técnicas Blackhat SEO (técnicas para el posicionamiento en buscadores), los atacantes pueden situar páginas maliciosas en los primeros lugares de las listas de resultados mostrados por los motores de búsqueda. A partir de ese momento, si el usuario hace clic en un enlace malicioso, será redirigido a la página de un falso antivirus en un dominio diferente. Dichas páginas tienen un aspecto muy real (ver imagen 1); De hecho, parece que un antivirus real está analizando el ordenador del usuario. El malware advierte al usuario de que su ordenador está infectado, y le anima a descargar un antivirus gratuito para limpiar la máquina.

Las páginas maliciosas se añaden demasiado tarde y muchas de ellas faltan. Del mismo modo, las herramientas antivirus tampoco sirven de mucho; de media, sólo 14 de las 41 herramientas más populares detectan el ejecutable como un virus (Kaspersky, AVG, McAfee, Fortinet, etc. no lo detectan). Por último, las herramientas de seguridad offline tampoco son la respuesta, ya que la redirección a la página del falso antivirus sólo se produce realizando una búsqueda online en Google/Yahoo/Bing.

LA SOLUCIÓN PANDA CLOUD INTERNET PROTECTION (PCIP)

Las amenazas dinámicas como los falsos antivirus requieren de la inspección online de todos los archivos: HTML, Javascript, etc. Además, para resultar efectivas, las soluciones de seguridad deben inspeccionar los contenidos en tiempo real. Mediante el análisis de todas y cada una de las transacciones online, el servicio de Amenazas Avanzadas de PCIP consigue detectar y bloquear las páginas de falsos antivirus que no estén incluidas en listas negras de terceros como Google Safe Browsing (parte de Firefox), malwaredomainlist.com, etc. La tecnología de inspección profunda ayuda a proteger de forma continua a las organizaciones ante las nuevas páginas y dominios de falsos antivirus que van apareciendo.

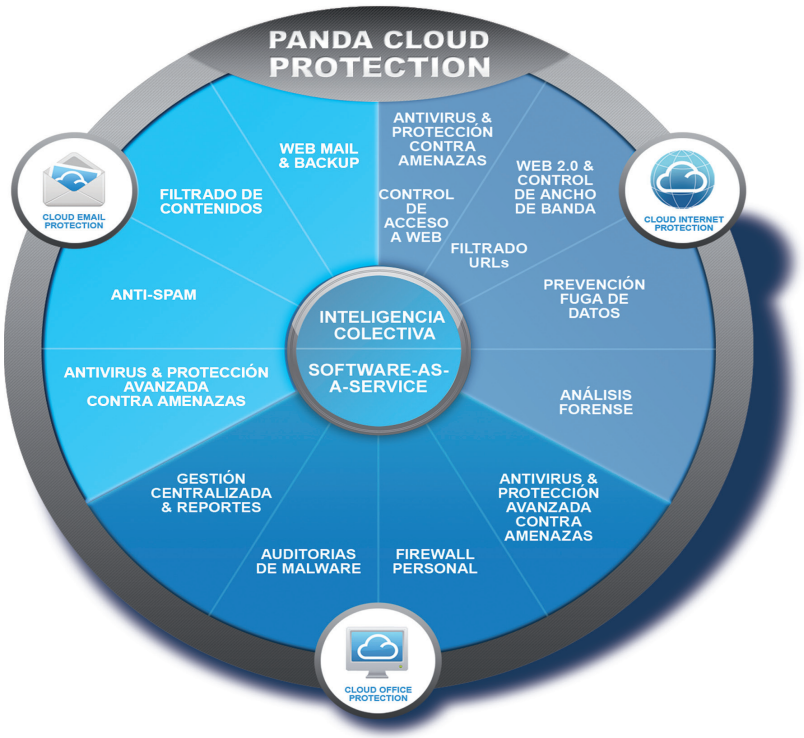
SUITE PANDA CLOUD PROTECTION

Panda Cloud Internet Protection es parte de la suite Panda Cloud Protection, una completa solución de seguridad SaaS que protege los principales puntos de entrada de las amenazas - endpoints, correo electrónico y tráfico Web- contra el malware, spam, cross-site scripting y otros ataques avanzados de We
ligera, segura y ser

Esta suite de seguridad está basada en la nube, ofreciendo máxima protección, reduciendo el gasto y aumentando la productividad. La solución se despliega en cuestión de minutos y se gestiona de forma sencilla gracias a la intuitiva Consola de Administración en la Nube única de Panda.

La suite Panda Cloud Protection se beneficia de la gran capacidad de la Inteligencia Colectiva: un sistema basado en la nube que almacena 2terabytes de conocimiento y experiencia obtenidos directamente de millones de usuarios. Panda Cloud Protection ofrece protección completa para el mundo real, no intrusiva e instantánea contra el malware conocido y desconocido.

Panda Cloud Protection explota el poder de la nube y proporciona protección en tiempo real contra las amenazas conocidas y desconocidas en cualquier momento y en cualquier lugar, gracias a su Consola de Administración en la Nube.



PANDA SECURITY

EUROPE
Ronda de Poniente, 17
28760 Tres Cantos. Madrid. SPAIN

Phone: +34 91 806 37 00

USA
230 N. Maryland, Suite 303
P.O. Box 10578. Glendale, CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com

© Panda Security 2010. All rights reserved. 0810-WP-Outdated Browsers

PANDA SECURITY