

Troyanos y Gusanos

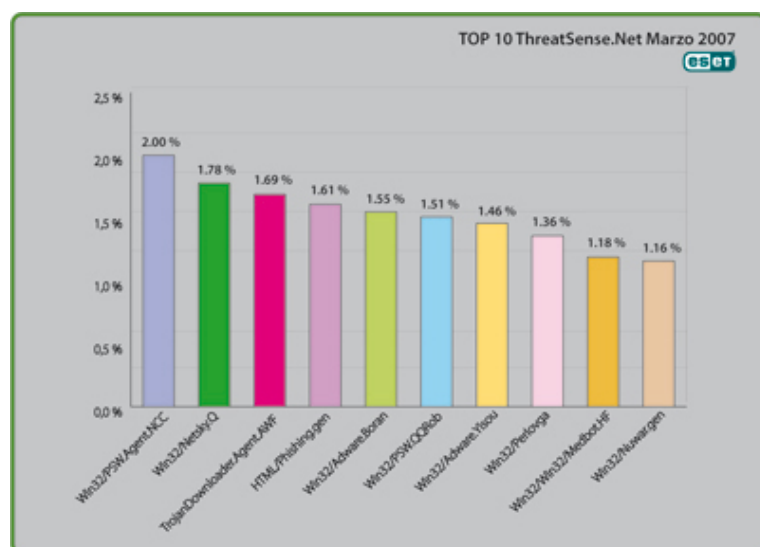
Ranking de ESET de Marzo: troyanos y gusanos continúan en la cima

Según la compañía ESET, el gusano Win32/PSW.Agent.NCC ocupa el primer lugar del ranking estadístico generado por su servicio ThreatSense.Net.

El Win32/PSW.Agent.NCC ocupa la primera posición del ranking de detecciones del mes de marzo elaborado por la empresa ESET a través del servicio estadístico ThreatSense.Net.

ThreatSense.Net es el servicio de Alerta Temprana de ESET NOD32 Antivirus, el cual indica el porcentaje de propagación de todos los códigos maliciosos que han sido detectados en los ordenadores de todo el mundo que tengan activado este servicio en su antivirus ESET NOD32. Los datos son enviados desde más de 10 millones de equipos únicos, que recogen estadísticas sobre más de veinte mil tipos distintos y familias de códigos maliciosos activos durante el último mes.

El PSW.Agent.NCC es un password stealer con características de keylogger y se encuentra en la primera posición del ranking con el 2% de las detecciones. Esta amenaza puede captar usuarios y contraseñas de cualquier servicio dentro del equipo infectado.



Este tipo de amenaza tiene como objetivo apropiarse de los datos personales del usuario (comerciales y/o financieros) para posteriormente causarle daño económico.

Esta tendencia de apropiarse de dinero indebido se mantiene debido a la aparición constante de nuevos malware que utilizan dichos métodos y, también, a través del aumento de phishing. Un ejemplo lo podemos observar en el PSW.Agent.NCC que sobrepasó al Win32/Nuwar.gen.

En la segunda posición, aparece el tradicional Netsky.Q, también conocido como Netsky.P por otras empresas, con más del 1,78%. Este gusano es capaz de reproducirse por correo electrónico y puede utilizar aplicaciones de intercambio de archivos (P2P) y recursos compartidos del equipo afectado.

Con el 1,69% del total se encuentra el Win32/TrojanDownloader.Agent.AWF. Esta amenaza es un troyano utilizado para descargar otros malware desde la Web. Normalmente el objetivo de éste es formar redes de equipos zombies conocidas como botnets para el envío masivo de spam y la realización de ataques distribuidos de denegación de servicios.

En la cuarta posición se sitúa el Phishing con el 1,61%. Esta amenaza se conforma de mensajes de correo electrónico, falsificados con la intención de engañar a usuarios crédulos para que revelen sus números de tarjetas de crédito, den información de sus depósitos de cuentas bancarias y todo tipo de detalles personales. Para los usuarios que caen en esta trampa los daños mayores son la pérdida total o parcial de su dinero en la cuenta bancaria o la tarjeta de crédito.

El Win32/Adware.Boran, ocupa el quinto lugar y se encarga por una parte de mostrar en la pantalla una ventana de publicidad y por la otra, también redirecciona al usuario a páginas Web especificados por el malware.

En la sexta posición aparece el Win32/PSW.QQRob, que recoge datos que el usuario introduce en su ordenador a través del teclado. Esta amenaza guarda todo lo que el usuario escribe, incluido claves y contraseñas de cualquier tipo, y luego se las envía por correo electrónico al creador del malware.

En el séptimo lugar encontramos el Win32/Adware.Yisou con casi el 1,50% de las detecciones totales. Este código malicioso es un adware asiático que viene teniendo un alto nivel de propagación.

En las últimas posiciones se encuentran muy variados códigos maliciosos, como el Win32/Perlovga, Win32/Medbot.HF y el Nuwar.gen.

Como puede verse claramente con la gran diversidad de los códigos maliciosos presentes en los ranking mensuales y el anual, las técnicas utilizadas por los creadores de malware son muy variadas. Sin embargo, se puede ver una clara tendencia a la explotación y utilización de la Ingeniería Social como principal técnica de propagación. También puede destacarse que la gran mayoría de las amenazas tienen un claro objetivo dirigido a los datos personales.

Por estos motivos, es de vital importancia que el usuario utilice herramientas de protección antivirus preactiva, así como su formación, ya que el uso seguro de los sistemas junto a software contra amenazas informáticas de calidad, garantiza una mejor y eficaz protección contra el malware.

© Eset, 2007

Fecha artículo: 2007-04-02 14:21:41 - url artículo: <http://www.internautas.org/html/4151.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org