



## LA INFECCIÓN DE UN PC ZOMBIE PUEDE DURAR MÁS DE DOS AÑOS, SEGÚN UN INFORME DE TREND MICRO

**Bogotá, 06 de Noviembre de 2009** – En un primer momento, los expertos de la industria estimaron que el tiempo medio que un equipo informático permanecía infectado era de 6 semanas. Sin embargo, un **reciente informe de Trend Micro** pone de manifiesto que esta estimación está lejos de ser exacta.

Así, durante el análisis de más de 100 millones de direcciones IP comprometidas Trend Micro ha identificado que el pico de IPs infectadas -direcciones que pertenecen a botnets o redes zombie- (o que son infectadas repetidamente) permanecen en este estado durante más de 2 años, aunque la media de infección es de 300 días en los principales países.

El término **botnet o red zombie** se utiliza para designar a los computadores que forman parte de una red robot tras haber sido infectados por algún tipo de Código Malicioso. Estos equipos pueden ser controlados por terceras personas con fines ilícitos (distribuir spam, robo de identidad, robo de información confidencial) sin que el usuario sea consciente de ello.

Según las estadísticas de Trend Micro, el 80% de todos los equipos comprometidos han estado infectados durante más de un mes. Lamentablemente, las noticias no consiguen mejorar. Pues mientras que el 75% de las direcciones IP comprometidas analizadas en el estudio han sido identificadas con usuarios particulares, el 25% restante pertenece a dominios de empresas. Debido a que una dirección IP para estos usuarios está generalmente identificada con un único gateway puede que, a su vez, esté conectada a varias máquinas en una red interna, lo que hace que el porcentaje actual de equipos empresariales afectados pueda ser más alto que las direcciones IP sugeridas en los datos –es decir, el porcentaje de PCs infectados en empresas es probablemente mucho más alto que ese 25%.

Una vez que el equipo pasa a estar comprometido, no es raro encontrar que se ha convertido en parte de una botnet más amplia. Las redes zombie con frecuencia causan daño en la forma de los ataques de malware, fraude, robo de información y otros crímenes. En lo que va de 2009, casi todo el malware rastreado por los expertos de Trend Micro está siendo utilizado por los cibercriminales para robar información (credenciales, etc.) principalmente.

Hasta ahora, las **tres redes zombie que son más peligrosas en relación con el robo de identidad**, información financiera y de cualquier otro tipo son:

- Koobface
- ZeuS/Zbot
- Ilomo/Clampi

## **100 millones de PCs en el mundo controlados por un grupo reducido de ciberdelincuentes**

En general, las botnets controlan más PCs comprometidos de lo que se pensaba hasta ahora. Sólo un “puñado” de delincuentes, probablemente unos cientos, tienen el control de más de 100 millones de equipos. Esto supone que los cibercriminales tienen mayor potencia de procesamiento a su disposición que todos los supercomputadores del mundo. De ahí que no resulte asombroso que **más del 90% de todos los correos electrónicos del mundo sea spam en la actualidad.**

Al día de hoy, no hay una correlación exacta de 1 a 1 entre los 10 países con más equipos infectados y los 10 principales países emisores de spam, sin embargo, sí es cierto que existen ciertas similitudes:

Utilizando **Koobface** como ejemplo de una red zombie típica, los expertos en amenazas de Trend Micro han establecido que **51.000 equipos comprometidos** actualmente forman parte de esta botnet particular. En cualquier momento, Koobface utiliza 5 o 6 comandos y centros de control (C&C) para controlar estos PCs infectados. Si un dominio C&C es dado de baja por un proveedor particular, los controladores de Koobface simplemente vuelven a registrar el mismo dominio C&C con otros proveedores. Entre mediados de marzo de 2009 y mediados del mes de agosto, Trend Micro registró unos 46 dominios C&C de Koobface.

En comparación, mientras se estudiaba la botnet **Ilomo**, se identificaron **69 dominios** C&C. Sin embargo, este número es difícil de confirmar cuando se añaden nuevos dominios mientras otros son eliminados a diario. Además, el número de equipos infectados dentro de la red zombie Ilomo no puede ser averiguado debido a la propia estructura de la botnet.

El equipo de expertos en amenazas de Trend Micro está comprometido con la investigación y análisis continuo. Los informes técnicos de las redes zombie Ilomo y Koobface han sido publicados y pueden consultarse en la sección de Investigación y Análisis de TrendWatch: <http://us.trendmicro.com/us/trendwatch/research-and-analysis/white-papers-and-articles/index.html>.

Afortunadamente, las nuevas tecnologías están disponibles para combatir este crecimiento de las amenazas. Tal es el caso de la tecnología **Trend Micro Smart Protection Network** que **evita que alrededor de 1.000 millones de amenazas infecten a los clientes de la compañía.**

Trend Micro emplea la potencia de **Smart Protection Network** para detectar y proteger contra los ataques. Esta infraestructura tecnológica está formada por 3 núcleos: **Reputación de Email, Reputación Web y Reputación de Archivos** combinadas con las técnicas de protección anti-spam y anti-malware para el puesto de trabajo más tradicionales.

Procesando casi 5.000 millones de peticiones de clientes al día, Trend Micro Smart Protection Network es la próxima generación de infraestructura de seguridad de contenidos para el cliente in-the-cloud diseñada para bloquear las amenazas antes de que éstas alcancen la red. Gracias a la combinación de tecnologías in-the-cloud con clientes más ligeros y pequeños, los usuarios tienen acceso inmediato a la seguridad más actualizada.

---

---

**Acerca de Trend Micro:**

*Trend Micro Incorporated, líder global en seguridad de contenido Internet, se enfoca en asegurar el intercambio de información digital para empresas y consumidores. Pionero y líder de la industria, Trend Micro está perfeccionando la tecnología integrada de administración de amenazas para proteger la continuidad operativa, la información personal y la propiedad contra el código malicioso, el spam, las fugas de datos y las amenazas Web más recientes. Visite TrendWatch en [www.trendmicro.com/go/trendwatch](http://www.trendmicro.com/go/trendwatch) para consultar más información sobre las amenazas. Las soluciones flexibles de Trend Micro, disponibles en múltiples factores de forma, cuentan con soporte 24/7 de expertos en inteligencia de amenazas alrededor del mundo. Una compañía transaccional, con oficinas corporativas en Tokio, las soluciones de seguridad confiables de Trend Micro se venden a través de sus socios comerciales en todo el mundo. Visite [www.trendmicro.com](http://www.trendmicro.com).*

---