El malware se protege a través de la dispersión geográfica

Un estudio publicado por **Blue Coat** arroja un poco de luz acerca de la persistencia de los ataques de malware a nivel mundial. Uno de los ejemplos destacables es el de la malnet **Shnakule** (red de malware) más grande de Internet, que utiliza entre 50 y 5.000 dominios cada día en función de la actividad y cuenta con servidores ubicados en 39 países a nivel mundial. Gracias a esta estructura en caso de que se desactiven los de alguna región, el malware sigue expandiéndose y lanzado los ataques pertinentes. Es lo que se denomina **protección por dispersión**.

Se trata de un proceso muy similar al de estructuras orgánicas como el **Pando**, una colonia de álamos localizada en América del Norte que comparte la misma raíz a pesar de que su extensión es de 43 hectáreas. En caso de que un tallo muera, este ecosistema hace brotar otros para mantenerse vivo. En la actualidad es el organismo más grande del mundo y se calcula que tenga 80.000 años de antigüedad. “La longevidad de Pando muestra lo difícil que es en última instancia acabar con una estructura tan difusa”, explica **Miguel Ángel Martos, Country Manager de Blue Coat en España y Portugal**.

Los operadores de malnets son capaces de transferir recursos de un lugar a otro en función de sus intereses. A comienzos de 2012, por ejemplo, sólo el 3% de los servidores de spam y scam de Shnakule se encontraba en Estados Unidos y Canadá. Seis meses después, este porcentaje ascendió al 40%

Para protegerse frente a la dispersión geográfica del malware, Blue Coat recomienda utilizar **técnicas de protección proactiva**, como la **Defensa de Día Negativo**. Básicamente, se trata de mantener el ritmo de protección y análisis continuamente, de tal forma que se pueden identificar las malnets que producen los ataques y bloquear los ataques en su origen en el momento en que se producen.

Blue Coat se basa en el servicio de defensa colaborativa **WebPulse**, capaz de identificar cualquier tipo de amenaza y almacenarla en una base de datos que crece cada segundo que pasa. Su arquitectura está diseñara para ser cada vez más inteligente: “Vale la pena saber lo que están haciendo las malnets, y adoptar un enfoque proactivo para asegurar los activos digitales. Al bloquear el mecanismo de distribución de las amenazas, en lugar de tratar de bloquear ataques específicos, la “Defensa de Día Negativo” protege a los usuarios con antelación a la implementación de los ataques”, finaliza Martos.