

El delito informático es más rentable que toda la industria antivirus

Thursday, 20 April 2006

El analista de virus Yuri Mashevsky, de Kaspersky Lab, ha publicado la segunda parte de un informe relacionado con el desarrollo de los códigos malignos durante 2005: "Malware Evolution: 2005, Part Two". A su juicio, los ciberdelincuentes obtienen un mayor beneficio con sus actividades que el conjunto de la industria antivirus mundial.

A juicio de Kaspersky Lab, los ciberdelincuentes obtienen un mayor beneficio con sus actividades, que el conjunto de la industria antivirus mundial.

El analista de virus Yuri Mashevsky, de Kaspersky Lab, ha publicado la segunda parte de un informe relacionado con el desarrollo de los códigos malignos durante 2005. "Malware Evolution: 2005, Part Two". Mashevsky concluye que la creación de virus, troyanos gusanos, ataques de negación de servicio, etc. se han convertido en una actividad industrial para ciberdelincuentes, y que esa actividad es incluso más lucrativa que la facturación de toda la industria antivirus.

Entre las tendencias que a juicio de Mashevsky destacaron especialmente en 2005 figura la confrontación más endurecida entre los ciberdelincuentes y la industria de la seguridad informática, como asimismo la confrontación entre distintos grupos de ciberdelincuentes. También menciona la tendencia a atacar servicios públicos, como consecuencia de que los ataques contra usuarios individuales no satisfacen las exigencias de rentabilidad de los atacantes.

Ciberdelincuentes contra la industria antivirus

Los delincuentes usan distintos métodos para atacar a la industria antivirus, observa Mashevsky. En tal sentido, indica que éstos realizan un intenso trabajo para identificar y eludir los nodos usados por las compañías antivirus para monitorizar el tráfico digital. Los ciberdelincuentes realizan ataques DoS organizados contra estos nodos, con el fin de dejarlos fuera de servicio por períodos de menor o mayor extensión. Esto tiene especial relevancia cuando intentan propagar un nuevo tipo de código maligno.

En la medida que las compañías de seguridad mejoran su capacidad de detección de código polimórfico -es decir código que se automodifica constantemente para evitar su identificación- los ciberdelincuentes buscan otros métodos para evitar que los virus sean revelados. Un método son los "multiple packers", es decir tecnología de compresión que permite ejecutar código e impedir a la vez que el proceso sea detectado por los sistemas antivirus.

Mashevsky menciona además que los ciberdelincuentes estudian atentamente las actualizaciones de todos los productos antivirus, ya que de esa forma saben cuales de sus códigos serán revelados.

Ciberdelincuentes contra ciberdelincuentes

Mashevsky menciona además que los ciberdelincuentes se atacan entre si en mayor medida que antes. Así, el código maligno de un grupo desactiva el código maligno de otro grupo, acompañado de amenazas recíprocas, al más puro estilo de la mafia. El experto da cuenta de nuevos métodos que hacen posible apoderarse de redes de computadoras zombi.

Al respecto, comenta que en noviembre de 2005 el control de una "botnet" determinada cambió de manos tres veces en el transcurso de un día. "Es más fácil raptar las redes de otros que establecer redes propias o comprarlas", Mashevsky.

El rango humano, o más bien calaña, de algunos ciberdelincuentes queda de manifiesto con el hecho de que no trepidan en usar acontecimientos de gran impacto público para distribuir su malware. Ejemplos en tal sentido son la distribución de código maligno relacionado con el huracán Katrina, los atentados de Londres, el tsunami asiático, etc.

La conclusión del experto es lapidaria: "Lo que ha ocurrido en 2005 no da razón alguna para sentirse optimistas respecto de la seguridad informática".