EL FUTURO NO PERTENECE A LOS ANTIVIRUS

Fausto Cepeda González

antivirus

numero-13

Los antivirus cumplieron en su época (finales de los ochenta) una labor importante para proteger satisfactoriamente a los equipos de cómputo. Sin embargo, el reinado de los antivirus tal cual los conocemos está llegando a su fin, en gran parte por su antiguo y ya no tan efectivo enfoque de listas negras. Hoy en día una empresa que desee seriamente proteger sus equipos de cómputo Windows contra los códigos maliciosos no debe permitir que su seguridad descanse únicamente en los antivirus.

Aunque no son nuevas y ya han estado de alguna forma viviendo en las infraestructuras de TI, (por ejemplo en productos que previenen intrusos en sistemas) las soluciones de listas blancas han evolucionado y están evidenciando la mejora indiscutible en su enfoque para proteger a los sistemas de los cientos de códigos maliciosos o sus variantes que aparecen cada día. Dicho enfoque es sencillo y supone un cambio sutil, pero que hace la diferencia: enlistar lo que está permitido ejecutarse en un sistema (lista blanca) *versus* enlistar lo que se prohíbe ejecutar en una computadora (lista negra usada por los antivirus).

Si tuviéramos únicamente un puñado de software malicioso (virus, troyanos, etc.), entonces implementar una lista negra sería relativamente sencillo y efectivo. Cada semana que apareciera un par de virus o gusanos obtendríamos su huella (con la cual sabríamos cómo identificarlos), generaríamos la firma correspondiente y actualizaríamos el antivirus. Ésta era la situación que se vivía en los noventa.

Hoy en 2012 es otra historia, los antivirus han demostrado su punto débil ante la abrumadora cantidad y poder del nuevo malware que hay que detener. Sin mencionar la pobre labor para detectar a los llamados APT (*Advanced Persistent Threat*), que por su naturaleza son avanzados (indetectables por los antivirus al usar técnicas evolucionadas) y persistentes (persiguen objetivos específicos y dirigidos, intentan incesantemente lograr sus metas).

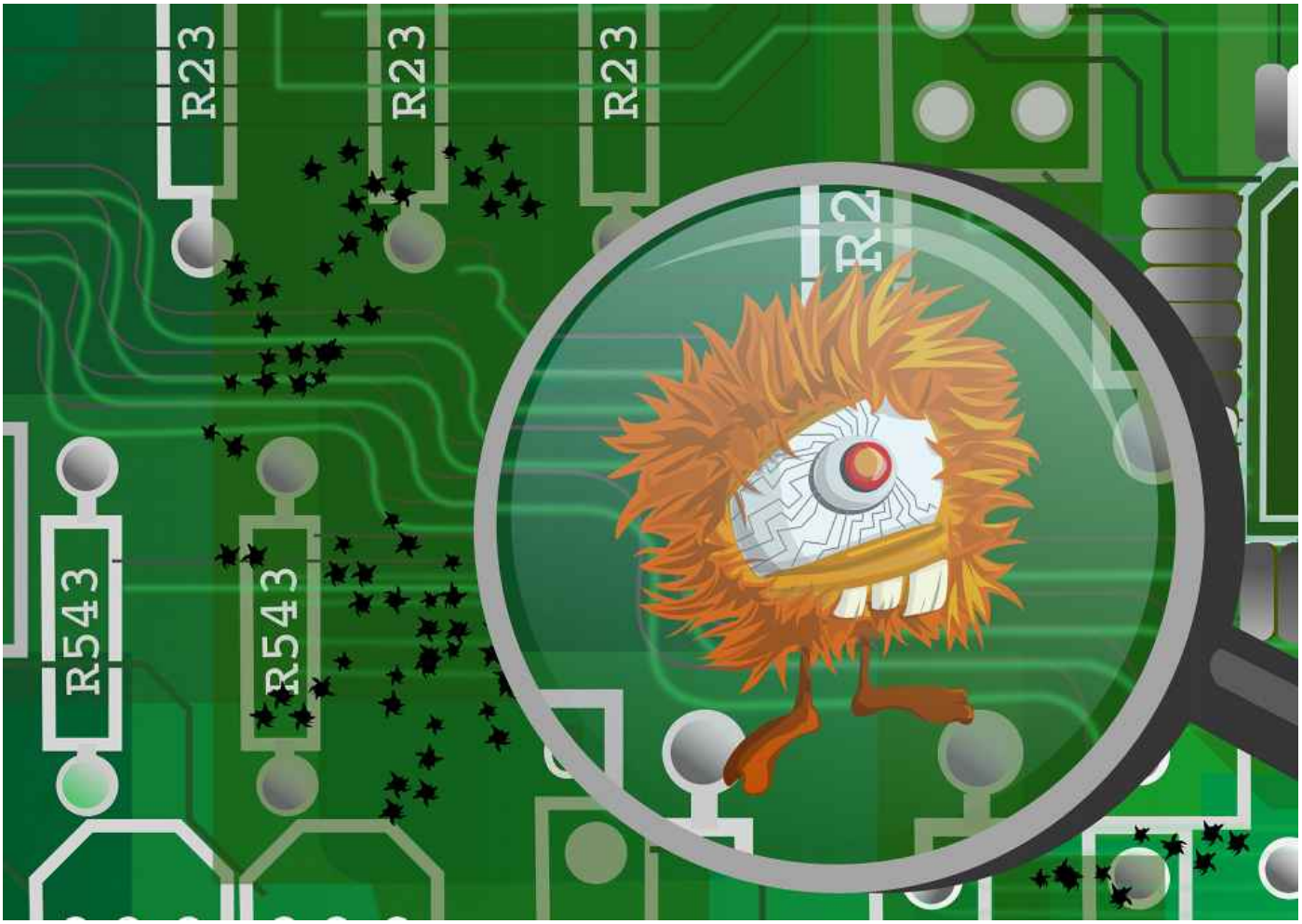
Los APT representan una amenaza que impacta usando un enfoque diferente al código malicioso común y corriente. Estos últimos siguen la estrategia de reproducirse en el mayor número de equipos posibles en un tiempo relativamente corto e infectar así a una base amplia de sistemas (así se construyen por ejemplo, las botnets, que son una colección de sistemas infectados bajo control del atacante). Ahora bien, los APT como los que afectaron a RSA o los que se vieron durante la llamada operación Aurora son específicos en el sentido de que se desea afectar a una empresa en particular. No hay un interés en comprometer masivamente a equipos (la detección de amenazas *masivas* es donde los antivirus tienen su nicho). Para los APT que usan estrategias avanzadas y específicas como

en el caso de StuxNet, los antivirus son burlados sin demasiada dificultad.

Ahora bien, uno podría pensar que al menos los antivirus proveen seguridad contra estos ataques genéricos donde se persigue una infección masiva. Sin embargo, aun en este escenario, la protección depende de que la compañía antivirus detecte al código malicioso, lo analice para generar la firma correspondiente y pueda empujarla a todos los clientes alrededor del mundo que tienen su producto. Es decir, transcurre un cierto tiempo entre que se identifica un virus y que finalmente nuestro antivirus cuenta con la firma apropiada para detectarlo y eliminarlo. Ese tiempo puede ser de horas o días, dependiendo de la rapidez para identificarlo, la prontitud para generar la firma y la importancia del *bicho* detectado, entre otros factores.

Cabe resaltar que los antivirus no se han quedado del todo estancados. Han mejorado diversas tecnologías usadas ya desde hace tiempo, como la llamada “heurística” que es una detección en base al comportamiento de archivos donde se trata de determinar si un ejecutable es potencialmente código malicioso nuevo.

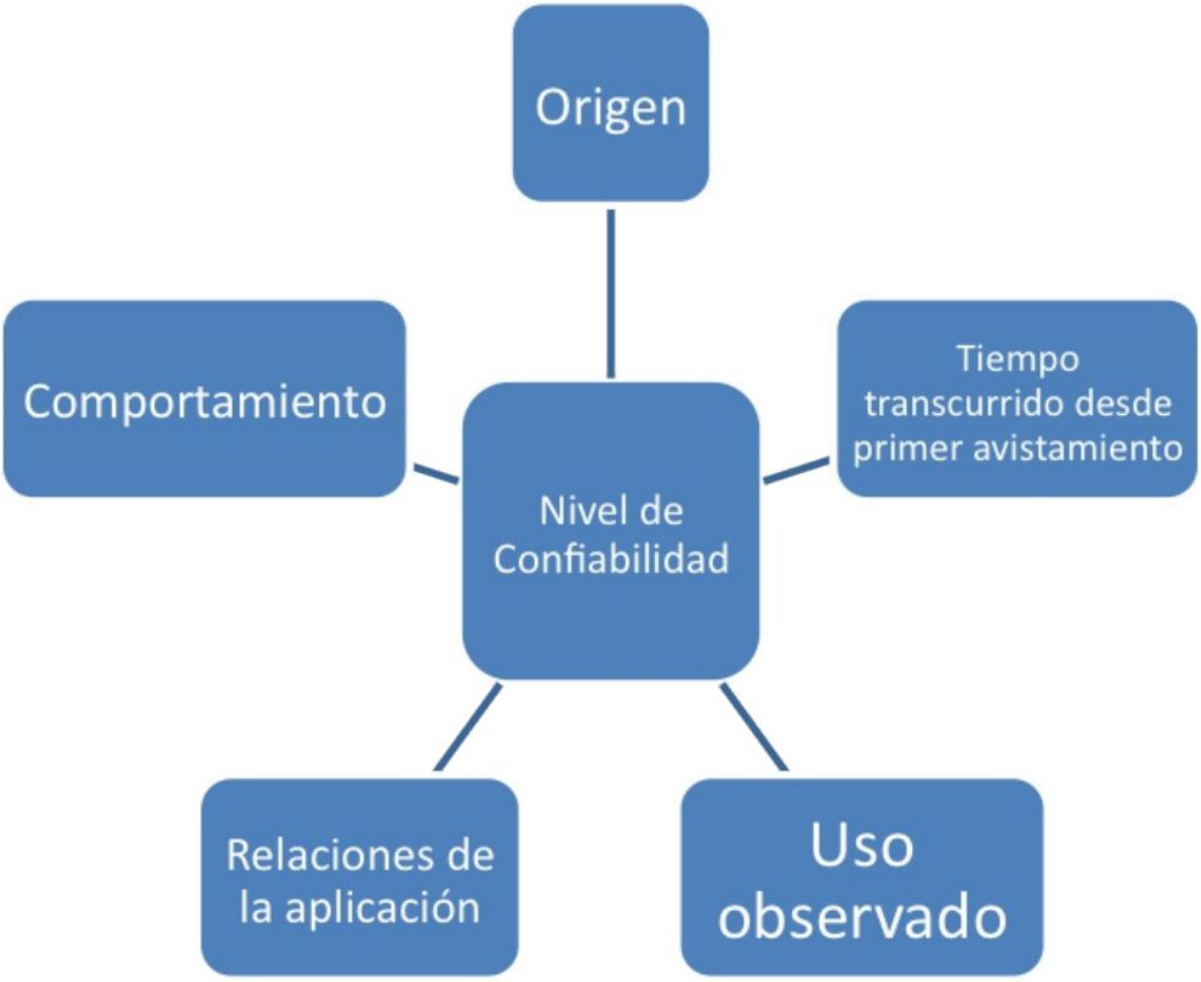
Otra mejora a introducido al usar la famosa nube, para mejorar la identificación y reducir los bytes de las firmas, además de acelerar la detección de nuevo código malicioso. De esta forma han ayudado ciertamente a atacar el problema. Sin embargo a) no están resolviendo la problemática de raíz y b) los equipos de cómputo continúan infectándose. Cualquier administrador de un antivirus corporativo podrá confirmar que con todo y las mejoras, los sistemas se siguen contaminando, lo que hace necesaria una limpieza manual en varios casos; algunos incluso llegan a recomendar que después de una infección, lo más apropiado sea formatear el equipo para reinstalar el sistema operativo.



Mientras los productos antivirus sigan requiriendo bajar diariamente actualizaciones de firmas, seguirá siendo evidente que la dependencia de éstas es un factor principal en su estrategia de detección. Lo anterior no solo se puede verificar en infraestructuras corporativas de TI donde frecuentemente aparecen infecciones en sistemas con antivirus actualizado, sino que también se han realizado pruebas donde se evidencia la contaminación exitosa de equipos que únicamente cuentan con este tipo de control basado en listas negras.

Las listas blancas no son un concepto nuevo, pero sí han madurado con el tiempo hasta llegar a convertirse en una solución suficientemente sólida como para ser usada en una corporación. Hace unos años estas listas blancas no eran un producto por sí solo sino que por lo general operaban junto con otra solución de seguridad. Trabajaban básicamente haciendo un *hash* de una aplicación y verificando que siempre que ésta solicitara *salida* a la red, contara con un *hash* válido. Y ciertamente, esta manera primitiva de administración no era nada cómoda para el administrador, quien tenía inicialmente que registrar cientos (o miles) de aplicaciones y averiguar si se podían catalogar como programas benignos. Pero la labor no termina ahí, ya que posteriormente se debían gestionar todos los cambios en las aplicaciones existentes (por ejemplo, por la aplicación de parches de seguridad o instalación de nuevas versiones) para darles el visto bueno y que pudieran seguir *saliendo* a la red, sin mencionar el registro de nuevas aplicaciones. Esto resultó ser un verdadero infierno administrativo y se optaba por hacer reglas genéricas, por lo tanto se reducía el poder para proveer seguridad.

El concepto no ha cambiado, pero sí la forma de administrar los registros de las listas blancas. Hoy en día existen soluciones más “inteligentes” en el sentido de que tratan de identificar por sí solas a las aplicaciones benignas, siguiendo ciertos criterios para establecer un “nivel de confiabilidad”, por ejemplo, cuánto tiempo se ha visto presente a esa aplicación en la infraestructura, si el programa proviene de una fuente confiable de la red corporativa (como un servidor de distribución de software) y otros parámetros, como se muestra a continuación:



Actualmente, se requiere tener dos soluciones separadas en las infraestructuras de TI, una de antivirus y otra de listas blancas, con toda la carga administrativa que eso conlleva: diferentes agentes instalados en los sistemas, un par de consolas de administración y servidores donde residen las soluciones. Es probable que en el futuro estas dos tecnologías converjan en un solo producto haciendo una labor preventiva (lista blanca) y reactiva (lista negra); de hecho algunas soluciones de listas blancas están tomando ya ese camino.

No sorprende que varias instituciones estén actualmente incorporando soluciones de listas blancas, como se ven el caso de la NSA en Estados Unidos. Cabe mencionar que existen diversas soluciones que podemos encontrar actualmente en el mercado y que están orientadas al control de aplicaciones por medio de listas blancas, por ejemplo:

· Bit9 con su producto “Parity Suite”.

· Lumension con su solución “Application Control” .

· CoreTrace con su lista blanca llamada “CoreTrace Bouncer”.

Las listas blancas vienen a llenar los huecos de los actuales controles basados en listas negras que luchan contra el código malicioso. Por lo tanto, el futuro cercano no debe seguir perteneciendo a los antivirus como el control por excelencia para proteger de los virus, gusanos, troyanos y códigos maliciosos en general. Una estrategia contra este tipo de amenaza ya no está completa sin la participación activa de un enfoque basado en listas blancas.
