El Boom de los Ataques de Malware: Fileless Malware

En cualquier estrategia de **concientización en ciberseguridad empresarial**, los empleados tienen un mandamiento esencial: nunca hay que abrir archivos adjuntos de un email si no se está completamente convencido de que es seguro. En caso contrario, su descarga o apertura puede provocar una crisis de seguridad informática en toda la empresa.

El Fileless Malware, también llamado **"malware sin fichero"**, se produce cuando el virus no entra en nuestro ordenador a través de un documento específico, sino que en realidad se instala dentro de la memoria RAM (principal de la computadora), pueden residir en el registro de Windows, o abusar de herramientas legitimas (como PowerShell, PsExec o Windows Management Instrumentation, entre otras).

El principal problema, y a diferencia de otros malware, es que no hay prácticamente soluciones de antivirus que sean capaces de limpiar este tipo de amenazas. Esta modalidad de ciberataque es especialmente peligrosa en el ámbito empresarial (que son los que manejan la información más valiosa y cuantiosa), ya que, al instalarse dentro de la memoria, el fileless malware ataca de manera más efectiva a través de **equipos que permanecen encendidos las 24 horas del día**, pudiendo llegar a alcanzar los servidores que afecten a toda la compañía provocando así una vulneración en cadena. Una vez ejecutado, esta técnica permite utilizar otras para infectar y aprovechar las vulnerabilidades de su huésped.

El Fileless Malware viene creciendo a pasos agigantados durante los últimos meses, y fácilmente se posiciona como una de las principales amenazas de seguridad para la próxima década. El bloqueo de estas amenazas se incrementó un 18% en comparación al semestre del 2018.

En cualquier caso, estos ataques pueden afectar a cualquier tipo de organización. Es justo lo que le pasó al Comité Nacional Demócrata de Estados Unidos a mediados de 2016, cuando un activista conocido como **Guccifer 2.0** insertó un malware sin archivo en su sistema y consiguió acceder a 19.252 correos electrónicos y 8.034 archivos adjuntos. Fruto de esta intrusión, Wikileaks publicó una serie de filtraciones que acabarían perjudicando a Hillary Clinton, por entonces rival de Donald Trump.

Información recolectada en páginas www.pandasecurity.com y www.itsecsas.com