16-05-2008

Más de 48 mil archivos de computadora colombiana fueron manipulados

ABN

La evaluación forense realizada por INTERPOL reveló que entre el 1 y 3 de marzo de 2008, 48.055 archivos fueron creados, abiertos, modificados o suprimidos por la policía de Colombia.

Así puede leerse en el párrafo 91, contenido en la página 33, del Informe Forense de Interpol sobre los Ordenadores y Equipos Informáticos de las Farc decomisados por Colombia.

Por si fuera fuera poco, 4.245 archivos tienen fechas futuras, que van desde el 5 de abril de 2009, hasta el 16 de octubre de 2010.

Dado su interés informativo, a continuación transcribimos textualmente el relato elaborado por Interpol:

79. Las autoridades colombianas encargadas de la aplicación de la ley comunicaron abiertamente a los especialistas de INTERPOL en investigación informática forense que un funcionario de su unidad antiterrorista accedió directamente a las ocho pruebas instrumentales citadas, en circunstancias
exigentes y marcadas por la premura de tiempo, entre el 1 de marzo de 2008, cuando fueron decomisadas por las autoridades colombianas, y el 3 de marzo de 2008.

80. Como se ha señalado anteriormente, los especialistas en informática de los organismos encargados de la aplicación de la ley pueden reconstruir lo ocurrido durante un acceso directo a pruebas electrónicas decomisadas, y eso han hecho los especialistas de INTERPOL en el curso de su examen forense.

81. De este modo, los especialistas de INTERPOL descubrieron lo siguiente:

82. Los sistemas operativos de los tres ordenadores portátiles decomisados mostraban que los tres ordenadores habían sido apagados el 3 de marzo de 2008 (a diferentes horas, pero todos ellos antes de las 11.4531, hora en que fueron entregados a los investigadores en informática forense de la policía judicial colombiana). Los dos discos duros externos y las tres llaves USB habían sido conectados a un ordenador entre el 1 y el 3 de marzo de 2008, sin que se hubieran obtenido previamente copias imagen forenses de su contenido y sin emplearse dispositivos de bloqueo de escritura (write-blockers).

83. En los archivos de la prueba instrumental decomisada no 26, un ordenador portátil, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 273 archivos de sistema
.-Apertura de 373 archivos de sistema y de usuario
.-Modificación de 786 archivos de sistema
.-Supresión de 488 archivos de sistema

84. En los archivos de la prueba instrumental decomisada no 27, asimismo un ordenador portátil, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 589 archivos de sistema

.-Apertura de 640 archivos de sistema y de usuario
.-Modificación de 552 archivos de sistema
.-Supresión de 259 archivos de sistema

85. En los archivos de la prueba instrumental decomisada no 28, igualmente un ordenador portátil, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 1.479 archivos de sistema
.-Apertura de 1.703 archivos de sistema y de usuario
.-Modificación de 5.240 archivos de sistema
.-Supresión de 103 archivos de sistema

86. En los archivos de la prueba instrumental decomisada no 30, un disco duro externo, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 1.632 archivos de sistema
.-Apertura de 11.579 archivos de sistema y de usuario
.-Modificación de 532 archivos de sistema
.-Supresión de 948 archivos de sistema

87. En los archivos de la prueba instrumental decomisada no 31, asimismo un disco duro externo, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 3.832 archivos de sistema
.-Apertura de 13.366 archivos de sistema y de usuario
.-Modificación de 2.237 archivos de sistema
.-Supresión de 1.049 archivos de sistema

88. En los archivos de la prueba instrumental decomisada no 32, una llave USB, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 8 archivos de sistema
.-Apertura de 12 archivos de sistema y de usuario
.-Modificación de 5 archivos de sistema
.-Supresión de 6 archivos de sistema

89. En los archivos de la prueba instrumental decomisada no 33, igualmente una llave USB, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 54 archivos de sistema
.-Apertura de 168 archivos de sistema y de usuario
.-Modificación de 28 archivos de sistema
.-Supresión de 52 archivos de sistema

90. En los archivos de la prueba instrumental decomisada no 34, también una llave USB, se presentaban los siguientes efectos producidos el 1 de marzo de 2008 o en fechas posteriores:

.-Creación de 1 archivo de sistema
.-Apertura de 60 archivos de sistema y de usuario
.-Modificación de 1 archivo de sistema

Conclusión no 3: INTERPOL no ha encontrado indicios de que tras la incautación a las FARC de las ocho pruebas instrumentales de carácter informático, efectuada el 1 de marzo de 2008 por las autoridades colombianas, se hayan creado, modificado o suprimido archivos de usuario en ninguna de dichas pruebas.

91. El acceso directo entre el 1 y el 3 de marzo de 2008 a las ocho pruebas instrumentales de carácter informático decomisadas a las FARC dejó rastros en los archivos de sistema, como ya se ha explicado.

No obstante, los especialistas de INTERPOL no encontraron en ninguna de las ocho pruebas archivo de usuario alguno que hubiera sido creado, modificado o suprimido con posterioridad al decomiso, practicado el 1 de marzo de 2008. Utilizando sus herramientas forenses, los especialistas hallaron un total de 48.055 archivos cuyas marcas de tiempo indicaban que habían sido creados, abiertos, modificados o suprimidos como consecuencia del acceso directo a las ocho pruebas instrumentales por parte de las autoridades colombianas entre el momento del decomiso de éstas, el 1 de marzo de 2008, y el 3 de marzo de 2008 a las 11.45 horas.

92. Los especialistas de INTERPOL descubrieron asimismo que uno de los ordenadores portátiles (prueba no 28) y los dos discos duros externos decomisados (pruebas no 30 y 31) contenían archivos cuyas marcas de tiempo eran erróneas, ya que indicaban una fecha futura.

93. La prueba no 28 contiene:
.-Un archivo cuya fecha de creación es el 17 de agosto de 2009

94. La prueba no 30 contiene:
.-668 archivos cuyas fechas de creación oscilan entre el 7 de marzo de 2009 y el 26 de agosto de 2009;
.-31 archivos cuyas fechas de última modificación varían entre el 14 de junio de 2009 y el 26 de agosto de 2009.
.-Estos archivos contienen música, vídeos e imágenes.

95. La prueba no 31 contiene:
.-2.110 archivos cuyas fechas de creación oscilan entre el 20 de abril de 2009 y el 27 de agosto de 2009;
.-1.434 archivos cuyas fechas de última modificación varían entre el 5 de abril de 2009 y el 16 de octubre de 2010

96. Basándose en el análisis de las características de estos archivos, los especialistas de INTERPOL concluyeron que estos archivos habían sido creados antes del 1 de marzo de 2008 en uno o varios dispositivos con una configuración de fecha y hora del sistema incorrecta. El hecho de que estos archivos aparezcan en las pruebas no 30 y no 31 indica que o bien fueron creados cuando dichas pruebas instrumentales se encontraban conectadas a un dispositivo con una configuración de fecha y hora del sistema incorrecta, o bien se transfirieron posteriormente (después de su creación), junto con sus respectivas marcas de tiempo de 2009, a las pruebas no 30 y no 31.

97. En lo que respecta al único archivo con fecha de creación de 2009 que contiene la prueba no 28, los especialistas de INTERPOL llegaron a la conclusión de que este archivo había sido primero creado y después transferido a la prueba no 28, y que su fecha de creación se había transferido con él.

98. Basándose en todo lo anterior, los especialistas de INTERPOL llegaron a la conclusión de que las autoridades colombianas no deberían tener en cuenta la fecha futura marcada en los archivos de las tres pruebas citadas (28, 30 y 31).

99. Habida cuenta de todo lo antedicho y habiendo realizado un examen forense exhaustivo, los especialistas de INTERPOL concluyen que no se ha creado, modificado o suprimido ningún archivo de usuario en ninguna de las ocho pruebas instrumentales de carácter informático después de su decomiso a las FARC, practicado el 1 de marzo de 2008.

Lea también:
+ Interpol no pudo asegurar que las computadoras fueran de Raúl Reyes