Hackers chinos han estado explotando una vulnerabilidad 0-day en el antivirus Trend Micro OfficeScan durante sus ataques contra Mitsubishi Electric, según confirmó ZDNet.

Trend Micro ya solucionó la vulnerabilidad, pero la compañía no ha comentado si el Zero Day se ha utilizado en otros ataques además de Mitsubishi Electric.

La información sobre los ataques a Mitsubishi se hicieron públicos el pasado lunes. En un comunicado de prensa, la compañía afirmó que fue hackeada el año pasado.

La empresa detectó una intrusión en su red el 28 de junio de 2019. Después de una investigación de algunos meses, Mitsubishi dijo que descubrió que los hackers obtuvieron acceso a su red interna desde donde robaron aproximadamente 200 MB de archivos.

En un inicio, la compañía no reveló el contenido de los documentos en un comunicado de prensa, pero dijo que los archivos contenían principalmente información acerca de los empleados, y no datos relacionados con sus negocios y socios.

Mitsubishi afirma que entre los documentos robados se encuentra:

- Datos sobre solicitudes de empleo para 1987 personas
- Resultados de una encuesta de empleados de 2012 que fue completada por 4566 personas de su oficina central
- Información sobre 1569 trabajadores de Mitsubishi Electric, que se jubilaron entre 2007 y 2019
- Archivos con materiales técnicos confidenciales corporativos, materiales de ventas, entre otros

Esta semana, medios japoneses informaron sobre el ataque cibernético. Según los informes, el pirateo se originó primero en una filial china de Mitsubishi Electric, luego se extendió a 14 departamentos y redes de la compañía.

Supuestamente, la intrusión se detectó luego de que el personal de Mitsubishi Electric

encontrara un archivo sospechoso en uno de los servidores de la compañía.

Nada de esto fue confirmado por la empresa japonesa. El único detalle técnico en relación con el hackeo que Mitsubishi Electric reveló fue el hecho de que los hackers explotaron una vulnerabilidad en uno de los productos antivirus que la compañía estaba utilizando.

Una fuente con conocimiento del ataque informó a ZDNet que los hackers explotaron la vulnerabilidad identificada como CVE-2019-18187, una vulnerabilidad de carga de archivos arbitraria y transversal del directorio en el antivirus Trend Micro OfficeScan.

Según un aviso de seguridad que Trend Micro envió en 2019, *«un atacante podría explotar las versiones afectadas de OfficeScan utilizando una vulnerabilidad transversal del directorio para extraer archivos de un archivo zip arbitrario a una carpeta específica en el servidor de OfficeScan, lo que podría conducir a la ejecución remota de código».*

Los diarios japoneses afirmaron que la intrusión fue resultado del trabajo de un grupo chino de espionaje patrocinado por el estado, conocido como Tick.

Tick es conocido por llevar a cabo muchas campañas de piratería dirigidas a objetivos en todo el mundo en los últimos años. Actualmente, no está claro si el grupo también usó el día cero de OfficeScan contra otros objetivos.