ANATOVA EL NUEVO RANSOMWARE QUE ESTA INFECTANDO EQUIPOS

Una nueva familia de **ransomware** descubierta a comienzos del 2019 ha generado alarma entre la comunidad de la ciberseguridad debido a sus aparentes funciones modulares y a sus desarrolladas técnicas de codificación, reportan especialistas en seguridad en redes del Instituto Internacional de Seguridad Cibernética.

Los investigadores han bautizado este ransomware como **'Anatova'**. A pesar de que no ha pasado siquiera un mes desde que fue identificado, el ransomware Anatova ya ha infectado cientos de computadoras en todo el mundo, reportan los especialistas en **seguridad en redes**. Según la investigación, los países con más infecciones de Anatova hasta el momento son Estados Unidos, Alemania, Francia y Bélgica.

Anatova se oculta utilizando el ícono de un juego o aplicación para que la víctima descargue el software malicioso. Si es descargado, instalado y ejecutado, Anatova es capaz de encriptar los archivos en la máquina comprometida, además de que puede encriptar archivos en redes compartidas, un escenario especialmente peligroso para las organizaciones más grandes.

Acorde a los especialistas en seguridad en redes, el ransomware Anatova utiliza el algoritmo Salsa20 para el cifrado, dejando de lado archivos de menos de 1 MB para atacar grandes empresas en una menor ventana de tiempo. El rescate que exigen los criminales consta de 10 unidades de criptomoneda Dash, cuyo valor se encuentra actualmente en alrededor de 700 dólares cada una.

Además, el ransomware esquiva el análisis a través de una serie de tácticas defensivas. Puede, por ejemplo, encriptar la mayoría de sus cadenas, usando múltiples claves de descifrado incrustadas en el archivo ejecutable. Incluso cuenta con una lista negra de usuarios, donde busca términos como 'tester', 'malware', o 'analyst'; si Anatova encuentra términos similares en el nombre de usuario, simplemente no se ejecuta.

Finalmente, el ransomware es capaz de limpiar cualquier registro de la memoria de la máquina con objeto de evitar que se descargue información que ayude a desarrollar programas para eliminar la encriptación.

Los investigadores destacan que Anatova fue diseñado para no infectar dispositivos ubicados en los países de la Comunidad de Estados Independientes (CIS), además de algunos territorios en Asia; en ocasiones esto puede brindar indicios sobre los autores de un software malicioso, aunque no es una regla que se cumpla sin excepción.