El ransomware FTCODE ha vuelto, con un nuevo conjunto de capacidades de robo de información dirigidas a navegadores y servicios de correo electrónico.

Este ransomware fue visto por primera vez en 2013, descubierto por Sophos. Se cree que es obra de grupos de hackers rusos y despertó el interés de los investigadores por su dependencia de PowerShell, un lenguaje de secuencias de comandos de Microsoft diseñado para la automatización de tareas y administración de redes.

Anteriormente, el ransomware se había dirigido a usuarios rusos, pero desde su creación, los operadores del malware ampliaron sus horizontes para incluir víctimas de otros idiomas.

En octubre de 2019, el ransomware se vinculó a campañas de phishing y correo electrónico dirigidas a usuarios italianos por medio de documentos que contienen macros maliciosas, una forma común para que los atacantes implementen kits de explotación.

Según investigadores de Zscaler ThreatLabZ, Rajdeepsinh Dodia, Amandeep Kumar y Atinderpal Singh, el malware ahora se está descargando por medio de VBScript, pero aún se basa en PowerShell.

> *«La campaña de ransomware FTCODE está cambiando rápidamente. Debido al lenguaje de secuencias de comandos en el que se escribió, ofrece múltiples ventajas a los actores de amenazas, permitiéndoles agregar o quitar funciones fácilmente o hacer ajustes mucho más fácilmente de lo que es posible con el malware tradicionalmente compilado»*, dicen los investigadores.

Lo que parece ser la última versión del malware, 1117.1, llega a las máquinas infectadas por medio del mismo vector de ataque: documentos que contienen macros. Sin embargo, estas macros contienen enlaces a VBScripts que implementan el FTCODE basado en PowerShell, disfrazado como un archivo de imagen señuelo .jpeg que aterriza en la carpeta %temp% de Windows.

FTCODE actúa como un ransomware típico. La información básica del sistema se envía a un servidor de comando y control (C2) en espera, y la persistencia se asegura por medio de un archivo de acceso directo en la carpeta de inicio que se ejecuta al reiniciar.

Después, FTCODE escaneará el sistema infectado en busca de unidades con al menos 50 kb de espacio libre y comenzará a cifrar archivos con extensiones que incluyen .das, .rar, .avi, .epk y .docx. Luego se publica la nota de rescate. Positive Technologies afirma que la solicitud inicial es de 500 dólares, pero aumenta con el tiempo.

La última versión del malware también es capaz de robar credenciales de navegador y correo electrónico, una actualización significativa en interacciones pasadas.

La información de los navegadores web Internet Explorer, Mozilla Firefox y Google Chrome, junto con las credenciales de correo electrónico de Microsoft Outlook y Mozilla Thunderbird, se pueden robar y enviar a los operadores del malware.

Los datos robados se cifran con el algoritmo base64 y se envían por medio de una solicitud HTTP POST, según Positive Technologies. Los investigadores agregaron que el ransomware también puede instalar el descargador JasperLoader, que se puede utilizar para implementar cargas maliciosas adicionales.