El Buró Federal de Investigaciones (FBI) de Estados Unidos, los Departamentos de Seguridad Nacional y Salud y Servicios Humanos (HHS), emitieron una alerta conjunta este miércoles en la que advierten de un aumento inminente de ransomware y otros ataques cibernéticos contra hospitales y proveedores de atención médica.

> *«Actores cibernéticos maliciosos se dirigen al sector Salud con el malware TrickBot, que a menudo conduce a los ataques de ransomware, robo de datos y la interrupción de los servicios de salud»,* dijo la Agencia de Seguridad e Infraestructura en un aviso.

La botnet por lo general se propaga por medio de correos electrónicos no deseados maliciosos a destinatarios desprevenidos, y puede robar datos financieros y personales, además de implantar otro software, como ransomware, en los sistemas infectados.

Cabe señalar que los ciberdelincuentes ya han utilizado TrickBot contra un importante proveedor de atención médica, Universal Health Service, cuyos sistemas fueron paralizados por el ransomware Ryuk a fines del mes pasado.

TrickBot también ha visto una interrupción importante en su infraestructura durante las últimas semanas, debido a que Microsoft orquestó un derribo coordinado para hacer inaccesibles sus servidores de comando y control (C2).

> *«El desafío aquí es debido a los intentos de eliminación, la infraestructura de TrickBot ha cambiado y no tenemos la misma telemetría que teníamos antes»,* dijo Alex Holden, de Hold Security.

Aunque el informe federal no hace mención de ningún actor de amenazas, el aviso toma nota del nuevo marco de puerta trasera Anchor de TrickBot, que recientemente se ha adaptado a Linux para apuntar a víctimas de más alto perfil.

> *«Estos ataques a menudo implicaban la exfiltración de datos de redes y dispositivos de punto de venta. Como parte del nuevo conjunto de herramientas Anchor, los desarrolladores de TrickBot crearon Anchor_DNS, una herramienta para enviar y recibir datos de las máquinas víctimas mediante la tunelización del Sistema de Nombres de Dominio (DNS)»*, dijo CISA.

Ayer informamos sobre Anchor_DNS, una puerta trasera que permite que las máquinas víctimas se comuniquen con los servidores C2 a través de un túnel DNS para evadir los productos de defensa de la red y hacer que sus comunicaciones se mezclen con el tráfico DNS legítimo.

Por otro lado, un informe separado de FireEye, ha nombrado a un grupo de amenazas con motivaciones financieras como UNC1878, que según los investigadores, han desplegado el ransomware Ryuk en una serie de campañas dirigidas contra hospitales, comunidades de jubilados y centros médicos.

Al instar al sector HPH a parchear los sistemas operativos e implementar la segmentación de la red, CISA también recomienda no pagar rescates, ya que esto puede alentar a los hackers a apuntar a organizaciones adicionales.

> *«Realice copias de seguridad de los datos, el espacio de aire y proteja con contraseña las copias de seguridad sin conexión. Implemente un plan de recuperación para mantener y retener múltiples copias de servidores y datos confidenciales o patentados en una ubicación segura y físicamente separada»,* dijo la agencia.