Investigadores de seguridad cibernética descubrieron una nueva versión del malware Sarwent, que abre los puertos RDP (Remote Desktop Protocol) en las computadoras infectadas para que los hackers puedan obtener acceso práctico a los hosts infectados.

Los investigadores de SentinelOne, creen que los operadores de Sarwent probablemente se están preparando para vender el acceso a estos sistemas en sitios web de piratería, un método común para monetizar hosts con capacidad RDP.

El malware Sarwent es un troyano de puerta trasera conocido que existe desde 2018. En sus versiones anteriores, el malware contaba con un conjunto limitado de funcionalidades, como la capacidad de descargar e instalar otro malware en las computadoras comprometidas.

Sin embargo, en una campaña detectada en las últimas semanas, el analista de malware de SentinelOne, Jason Reaves, afirma que Sarwent recibió dos actualizaciones críticas.

Entre las nuevas características, destaca su capacidad de ejecutar comandos de CLI personalizados por medio del Símbolo del Sistema de Windows y las utilidades de PowerShell.

Aunque esta nueva característica es muy intrusiva por sí sola, el investigador afirma que Sarwent también recibió otra nueva característica con la actualización.

Reaves afirma que Sarwent ahora registra una nueva cuenta de usuario de Windows en cada host infectado, habilita el servicio RDP y luego modifica el firewall de Windows para permitir el acceso RDP externo al host infectado.

Esto significa que los operadores de Sarwent pueden utilizar el nuevo usuario de Windows que se crea para acceder a un host infectado sin ser bloqueado por el firewall local.

Reaves dijo en una entrevista con ZDNet, que la distribución de la nueva versión de Sarwent es limitada hasta ahora.

> *«Solo he visto esta nueva versión descargada como una infección secundaria a otro malware, por ejemplo, Predator the Thief»*, dijo Reaves.

Debido al esquema de configuración actual, limpiar una infección de Sarwent es *«un poco más complicado».* Esto incluye la eliminación de Sarwent, el malware original que lo instaló, eliminar al nuevo usuario de Windows y después cerrar el puerto de acceso RDP en el firewall de Windows.

Hasta el momento, es un misterio saber qué hace el malware con el acceso RDP que obtiene en los hosts infectados.

> *«Normalmente, el desarrollo de malware en el dominio de crimeware está determinado por el deseo de monetizar algo o por la demanda de funcionalidad de los clientes»,* dijo Reaves.

Enre algunas teorías, puede suceder que los actores detrás de Sarwent utilicen el acceso RDP ellos mismos, para robar datos patentados o instalar ransomware, o pueden alquilar el acceso RDP a otros hackers. Otra opción, es enumerar los puntos finales RDP en las denominadas *«tiendas RDP»*.

Los indicadores de compromiso (COI) para la nueva versión de malware Sarwent se incluyen en el informe Sarwent de SentinelOne. Los equipos de seguridad pueden usar estos COI para buscar infecciones de Sarwent en sus flotas de computadoras.