El malware Racoon Stealer como plataforma de servicio ganó notoriedad hace algunos años por su capacidad para extraer datos almacenados en navegadores web. Estos datos incluían inicialmente contraseñas y cookies, que a veces permiten autenticar un dispositivo reconocido sin ingresar una contraseña.

Racoon Stealer también fue diseñado para robar datos de autocompletar, que pueden incluir una gran cantidad de información personal que va desde datos de contacto básicos hasta números de tarjetas de crédito. Además, Racoon Stealer también tenía la capacidad de robar criptomonedas y robar o añadir archivos en un sistema infectado.

Por lo malo que haya sido Racoon Stealer, sus desarrolladores crearon recientemente una nueva versión que está diseñada para ser mucho más dañina que la versión anterior.

Nuevas capacidades de Racoon Stealer

La nueva versión de Racoon Stealer aún tiene la capacidad de robar contraseñas del navegador, cookies y datos de autocompletar. También tiene la capacidad de robar cualquier número de tarjeta de crédito que esté guardado en el navegador.

Además, la última versión de Racoon Stealer es mucho más capaz que su predecesora cuando se trata de robar criptomonedas. Racoon Stealer no solo puede atacar billeteras de criptomonedas, sino que también tiene la capacidad de atacar numerosos complementos de navegador relacionados con criptomonedas.

Los desarrolladores de Racoon Stealer también mejoraron la capacidad del malware para recopilar datos de archivos. Mientras que la versión anterior finalmente se mejoró para permitir el robo de archivos individuales, la última versión es capaz de robar archivos independientemente del disco en el que residan.

Además, la nueva versión de Racoon Stealer puede capturar una lista de las aplicaciones que están instaladas en la máquina, lo que puede ser útil para ayudar a un atacante a saber qué tipos de archivos de datos pueden existir y vale la pena robar.

Algo inquietante es que Racoon Stealer puede realizar capturas de pantalla de un sistema infectado. Las capturas de pantalla podrían usarse para una innumerable variedad de propósitos maliciosos.

Por ejemplo, un atacante posiblemente podría ver a alguien ingresar información de pago relacionada con la compra y tomar una captura de pantalla de la pantalla de pago, capturando así no solo un número de tarjeta de crédito, sino todos los detalles de respaldo que podrían ser necesarios para usar la tarjeta de crédito.

Cabe mencionar que una función de captura de pantalla podría usarse para robar cualquier tipo de datos confidenciales y un atacante que haya creado dicha captura podría usarla como base para un plan de extorsión cibernética.

¿Cómo proteger una organización?

Defenderse de esta última versión de Racoon Stealer se reduce en gran medida a adherirse a las mejores prácticas de seguridad establecidas desde hace mucho tiempo. Por ejemplo, nunca se debe hacer clic en un enlace o abrir un archivo adjunto dentro de un mensaje, a menos que se conozca el remitente.

Incluso al conocer el remitente, es importante tomarse el tiempo para verificar la autenticidad de un mensaje antes de hacer clic en cualquier enlace o abrir archivos adjuntos.

También es muy importante mantener su sistema operativo y aplicaciones actualizados con los últimos parches de seguridad. Del mismo modo, se debe evitar ejecutar aplicaciones obsoletas que ya no se actualizan. Esto es especialmente cierto para los navegadores, ya que es el objetivo principal de Racoon Stealer.

Es necesario asegurarse de tener instalada la protección contra malware en todos sus sistemas y de que esta protección contra malware se mantenga actualizada.