La compañía de inteligencia de riesgos cibernéticos con sede en Atlanta, Cyble, descubrió un nuevo malware troyano de acceso remoto (RAT), al que denominaron Borat.

El malware RAT por lo general ayuda a los hackers a obtener el control completo del sistema de una víctima, permitiéndoles acceder a los recursos de la red, archivos y poder alternar el mouse y teclado.

El malware Borat RAT va más allá de las características estándar y permite a los atacantes implementar ransomware y ataques DDoS. También aumenta la cantidad de actores de amenazas que pueden lanzar ataques, a veces apelando al mínimo común denominador.

La funcionalidad añadida de llevar a cabo ataques DDoS hace que sea insidioso y un riesgo para las organizaciones digitales de hoy.

El ransomware ha sido el tipo de ataque principal más común durante más de tres años. Según un informe de IBM, REvil fue la variedad de ransomware más común y consistió en aproximadamente el 37% de todos los ataques de ransomware. Borat RAT es una combinación única y poderosa de capacidades RAT, spyware y ransomware fusionadas en un solo malware.

Borat RAT: ¿Por qué es una triple amenaza?

Borat RAT proporciona un tablero para que los hackers maliciosos realicen actividades de malware RAT y la capacidad de compilar el binario de malware para ataques DDoS y ransomware en la máquina de la víctima. La RAT también incluye código para lanzar un ataque DDoS, ralentiza los servicios de respuesta a usuarios legítimos e incluso, puede hacer que el sitio se desconecte.

De forma sorprendente, Borat RAT puede entregar una carga útil de ransomware a la máquina de la víctima para cifrar los archivos de los usuarios y exigir un rescate. El paquete también incluye un archivo ejecutable keylogger que monitorea las pulsaciones de teclas en las computadoras de las víctimas y las guarda en un archivo .txt para su exfiltración.

Las otras funcionalidades del malware Borat RAT que lo hacen interesante incluyen:

- Un proxy inverso para proteger al hacker
- La capacidad de robar credenciales de navegadores o tokens de Discord
- Introducir código malicioso en procesos legítimos

Por otro lado, con el fin de molestar a las víctimas, Borat RAT también puede hacer:

- Apagar y encender el monitor
- Ocultar/mostrar las funciones del escritorio, como el botón de inicio y la barra de tareas
- Reproducción de audio no deseado
- Encender/apagar la luz de la cámara web

El malware Borat RAT verificará si el sistema tiene un micrófono conectado y, de ser así, grabará el audio de la computadora, que se guardará en otro archivo llamado «*micaudio.wav*«. De forma similar, el malware puede comenzar a grabar desde la cámara si se descubre una cámara web en el sistema.

Es necesario que las empresas tomen accesiones de seguridad para evitar que los empleados dejen entrar ransomware a una organización, aún cuando sea sin saberlo y por error. Para esto es necesario crear un plan de buenas prácticas donde se incluyan las acciones a seguir al momento de utilizar unidades extraíbles en los equipos de cómputo, o al abrir correos electrónicos.