Google está emitiendo una advertencia acerca de varios actores de amenazas que están compartiendo un exploit de prueba de concepto (PoC) público que aprovecha su servicio de Calendario para alojar una infraestructura de comando y control (C2).

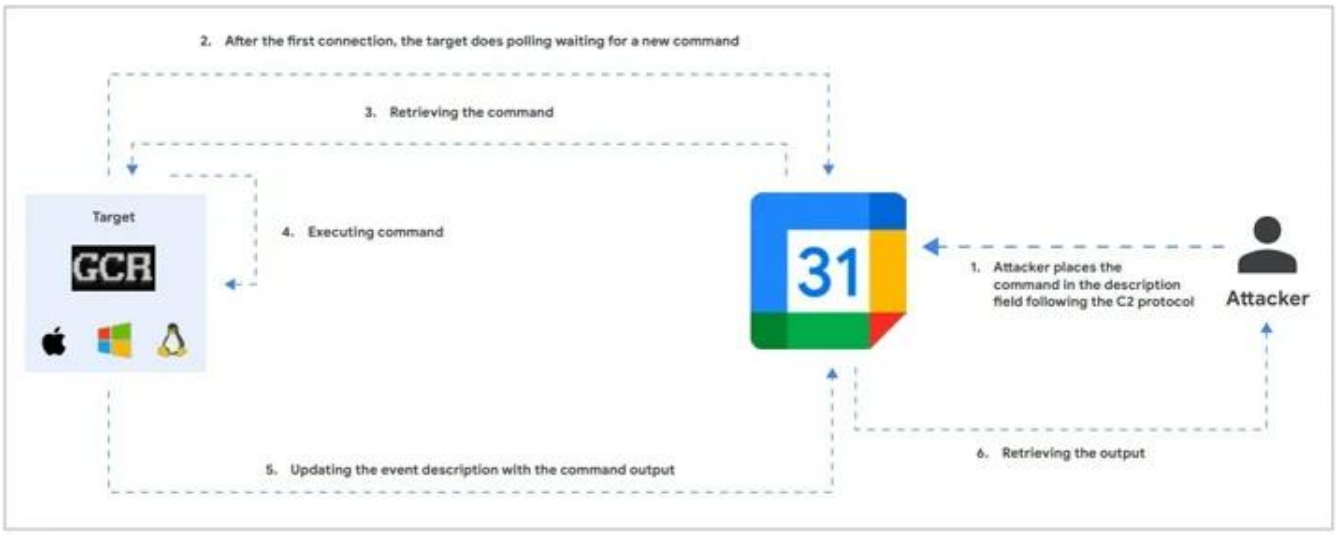
La herramienta, conocida como Google Calendar RAT (GCR), utiliza Eventos del Calendario de Google para C2 a través de una cuenta de Gmail. Esta herramienta fue publicada por primera vez en GitHub en junio de 2023.

> El desarrollador e investigador, que utiliza el seudónimo en línea MrSaighnal, explica que *«el script crea un 'Canal Encubierto' al explotar las descripciones de eventos en el Calendario de Google. El objetivo se conectará directamente a Google».*

En su octavo informe de Threat Horizons, la gigante tecnológica informa que no ha observado el uso de esta herramienta en el mundo real, pero señala que su unidad de inteligencia de amenazas, Mandiant, ha detectado que varios actores de amenazas comparten el PoC en foros clandestinos.

> Google describe el funcionamiento de GCR de la siguiente manera: *«GCR, funcionando en una máquina comprometida, sondea periódicamente la descripción del evento del Calendario en busca de nuevos comandos, ejecuta dichos comandos en el dispositivo objetivo y luego actualiza la descripción del evento con la salida de los comandos».*

La particularidad de esta herramienta es que opera exclusivamente en infraestructura legítima, lo que dificulta que los defensores detecten actividades sospechosas, según Google.



Google Calendar RAT attack flow diagram, published by the developer on Github

Este desarrollo resalta el interés continuo de los actores de amenazas en abusar de los servicios en la nube para integrarse en los entornos de las víctimas y pasar desapercibidos.

Esto incluye a un actor estatal iraní que fue visto empleando documentos con macros para comprometer a usuarios con un pequeño backdoor .NET apodado BANANAMAIL para Windows, que utiliza el correo electrónico para el comando y control.

Google informa que su Grupo de Análisis de Amenazas ha desactivado las cuentas de Gmail controladas por el atacante que se utilizaron como conducto para el malware.