Google Cloud

Horizonte de Amenazas Cibernéticas

Informe de amenazas cibernéticas | Segundo semestre 2024

Oficina del CISO

Índice

Declaración de misión

El informe Horizonte de Amenazas Cibernéticas de Google Cloud ofrece a los responsables de tomar decisiones información estratégica sobre amenazas que afectan no solo a Google Cloud, sino a todos los proveedores. El informe se centra en recomendaciones para mitigar los riesgos y mejorar la seguridad en la nube dirigida a líderes y profesionales del área. El informe incluye insights del Grupo de Análisis de Amenazas (TAG) de Google, Mandiant, la Oficina del CISO de Google Cloud, el área de Ingeniería de Seguridad de Productos, y varios equipos de inteligencia, seguridad y productos de Google Cloud.

Resumen ejecutivo

Equipando a los protectores de la nube con medidas de seguridad para la computación sin servidor

La computación sin servidor ha surgido como un enfoque transformador para el desarrollo de aplicaciones, prometiendo escalabilidad, menor sobrecarga operativa y un tiempo de salida al mercado más rápido.

Los productos sin servidor también generan oportunidades para los agentes de amenazas en proveedores de nube a partir de posibles errores de configuración de seguridad en los entornos de los clientes. ¿Qué significa esto para los profesionales de la seguridad en la nube?

En función de las recientes amenazas a la nube sin servidor que detectan nuestros equipos de seguridad e inteligencia, las siguientes son tres consideraciones clave a tener en cuenta en una estrategia de seguridad en la nube:

- **Credenciales en peligro:** los agentes de amenazas aprovechan contraseñas débiles para obtener acceso no autorizado a los proyectos de Google Cloud. Al mismo tiempo, la computación sin servidor puede hacer que la criptominería sea un objetivo aún más atractivo para algunos agentes, lo que subraya la importancia de los esfuerzos para identificar actividades sospechosas en entornos de nube.
- **Errores en la configuración:** nuestras investigaciones sobre detección y respuesta indican que es necesario garantizar prácticas recomendadas de seguridad sin servidor para ayudar a defenderse contra agentes de amenazas que buscan errores en la configuración.
- **Distribución de malware:** los agentes de amenazas aprovechan la tecnología sin servidor y ajustan las tácticas en respuesta a la detección previa por parte de los protectores de la red.

El informe Cybersecurity Forecast 2024 de Google Cloud predice que “los cibercriminales y los operadores cibernéticos de los estados nacionales aprovecharán en mayor medida las tecnologías sin servidor dentro de la nube porque ofrecen mayor escalabilidad y flexibilidad, y pueden implementarse mediante herramientas automatizadas”.

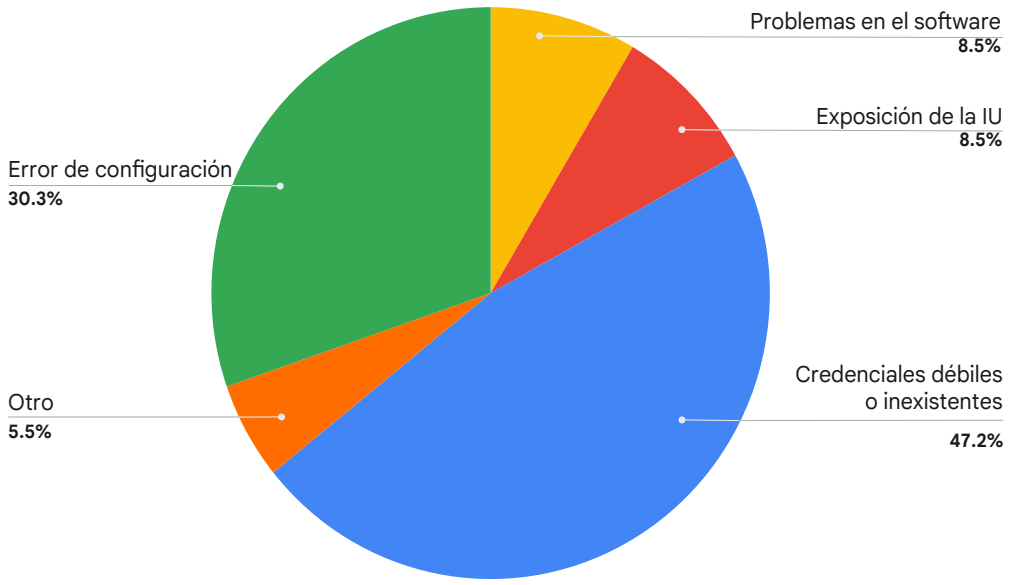
Hemos visto a los agentes de amenazas cumplir con esa predicción al explotar las brechas de seguridad de la computación sin servidor. Las siguientes secciones profundizan en las principales conclusiones de estas amenazas para mejorar las defensas de seguridad en la nube.

En cifras: los desafíos de identidad siguen siendo un riesgo para entornos sin servidor

Como parte del compromiso continuo de Google Cloud con la seguridad, la Oficina del CISO para la nube monitorea la actividad de incidentes y las tendencias asociadas con la forma en que los agentes de amenazas obtienen acceso no autorizado a los entornos de nube y a sus objetivos una vez dentro. Estos datos, junto con nuevos insights de la plataforma (de operaciones de seguridad de Google (anteriormente Chronicle), se pueden encontrar a continuación.

Google Cloud investigó los vectores de acceso iniciales en varias fuentes durante el primer semestre de 2024, analizando tanto las intrusiones exitosas en los entornos de los clientes como las posibles vulnerabilidades o brechas encontradas en los datos anónimos de la plataforma de operaciones de seguridad de Google para una gran base de clientes. Este enfoque nos permitió no solo evaluar cómo los agentes de amenazas ingresaron a los entornos de nube de los clientes en el primer semestre, sino también determinar qué áreas tienen el mayor potencial de crecimiento en seguridad para las organizaciones en el segundo semestre.

Vectores de acceso inicial que son motivo de preocupación (primer semestre 2024)



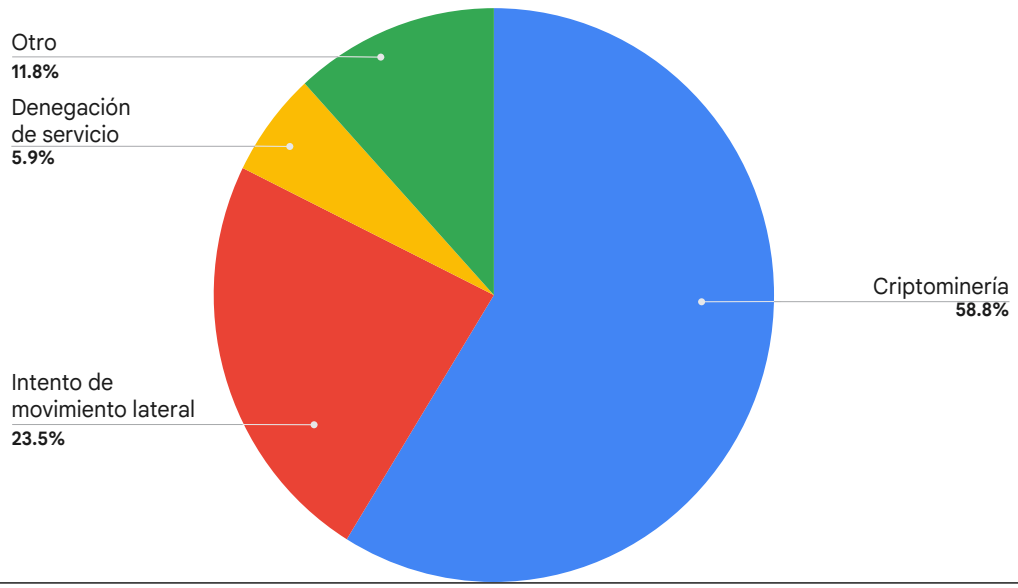
Las credenciales débiles o inexistentes siguieron siendo un factor clave de acceso inicial, lo que representa el vector de éxito más frecuente y el segundo desencadenante más común de las reglas de detección. Sin embargo, los errores de configuración aumentaron a más del 30%, en gran medida debido al alto volumen de detección de factores mal configurados en el entorno.

Si bien los agentes de amenazas no siempre aprovechan estos errores en las configuraciones, siguen siendo una puerta abierta para posibles actividades maliciosas. Un ejemplo de un problema común de mala configuración sería que las claves de cuentas de servicio tengan demasiados permisos o no cuenten con suficientes controles preventivos contra el uso malicioso. El riesgo que plantea la configuración incorrecta destaca un beneficio clave de la computación sin servidor, ya que minimiza la supervisión de la configuración necesaria para el mantenimiento del servidor de procesos críticos.

Además, estos hallazgos respaldan la relevancia de la arquitectura sin servidor como parte de una estrategia de defensa más amplia y profunda, como un control preventivo que acompaña a otros controles de detección implementados en caso de una posible intrusión para encontrar y detener a los atacantes en diversos puntos del proceso. La categoría “Otro” incluyó una serie de detecciones sospechosas, tales como herramientas de prueba de penetración que se infiltraron con éxito en las instancias e intentos de tunelización de DNS.

Los objetivos finales de las intrusiones fueron en gran medida los mismos durante el primer semestre de 2024, ya que casi el 59% de las intrusiones estuvieron motivadas por esfuerzos de criptominería, lo que es ligeramente inferior a nuestras observaciones del segundo semestre de 2023 (65%).

Impacto observado de la intrusión (primer semestre 2024)



Mitigaciones

- Muchos escenarios que utilizan claves de cuentas de servicio se pueden solucionar con métodos de autenticación más seguros tque no dependen de la descarga y distribución de archivos de claves. Además, Google Cloud utiliza políticas predeterminadas para reducir el riesgo que representan las amenazas a las claves de cuentas de servicio como parte de su arquitectura segura. Recomendamos evaluar y reducir el uso innecesario de estas claves con la guía que se encuentra aquí.
- Asegura la adopción total de la autenticación multifactor (MFA) para el acceso administrativo a aplicaciones web sin servidor, así como a otras instancias de Google Cloud.
- Las pruebas de penetración son necesarias para evitar que los agentes de amenazas utilicen herramientas de seguridad ofensivas básicas para acceder al entorno.
- Aprovecha la detección de amenazas de eventos de Security Command Center (SCC) de Google para identificar actividades sospechosas dentro del entorno de nube de la organización, tales como la generación inapropiada de tokens u observaciones de geolocalización anómalas. Aprovecha el programa de protección contra criptominería de SCC de Google para organizaciones elegibles.

Amenazas a las funciones y los servicios de backend sin servidor

La computación sin servidor ofrece ventajas innegables, pero la seguridad debe integrarse desde el principio. Al comprender el panorama de amenazas e implementar mitigaciones sólidas, las organizaciones pueden aprovechar las fortalezas de la computación sin servidor y, al mismo tiempo, proteger las aplicaciones, los datos y la infraestructura en la nube.

En lo que respecta a la respuesta a incidentes y las acciones proactivas durante los últimos dos años, Mandiant ha observado una multitud de amenazas a la arquitectura sin servidor en todos los proveedores de nube. Las siguientes amenazas deben ser prioridad al implementar u operar una arquitectura sin servidor:

- Secretos codificados y no codificados
- Atacantes que utilizan la infraestructura sin servidor con fines maliciosos
- Arquitectura y prácticas de desarrollo inseguras
- Servicios de backend mal configurados

Secretos codificados y sin codificar

Se debe evitar a toda costa la práctica de incorporar secretos, como claves de API y credenciales de bases de datos, directamente en el código de las funciones sin servidor o en variables de entorno. Por desgracia, esta práctica sigue estando muy extendida en las plataformas de nube, y Mandiant suele identificar secretos sin codificar durante la respuesta a incidentes y las interacciones proactivas con los clientes. Algunos de los principales riesgos son:

- **Exposición:** si tu código queda expuesto (filtración de repositorio, permisos mal configurados, entorno de alojamiento comprometido, etc.), los atacantes podrían obtener acceso a las credenciales sin codificar. Además, si un atacante puede obtener acceso de lectura a los recursos de la nube, podría acceder a las credenciales sin codificar almacenadas en el código de la función o en las variables. En ambos casos, esto podría permitir la asignación de privilegios dentro del entorno de nube o la capacidad de moverse lateralmente a otras plataformas o servicios.
- **Control de versiones:** los secretos en el código o en las variables del entorno a menudo quedan expuestos al control de versiones, lo que crea un riesgo a largo plazo, incluso si se soluciona la exposición inicial.
- **Rotación de credenciales:** los secretos codificados dificultan la rotación periódica de credenciales, que ayuda a limitar el daño potencial si se vulnera un secreto. Sin embargo, con estos secretos, la rotación de credenciales requiere modificar y volver a implementar la función, lo que genera una sobrecarga operativa y aumenta el riesgo de errores.

Mitigaciones y mejores prácticas

- **Secret Manager:** utiliza Google Cloud Secret Manager para guardar y administrar secretos de forma segura. Cloud Run se integra con Secret Manager para permitirte montar secretos como variables de entorno o archivos.
- **Nunca almacenes secretos directamente en variables de entorno:** los secretos almacenados directamente en variables de entorno no están cifrados y se puede acceder a ellos fácilmente. Cloud Run crea recomendaciones de forma proactiva si detecta variables de entorno que podrían ser contraseñas, claves de API o credenciales de aplicaciones de Google.
- **Principio de privilegio mínimo:** sigue el principio de privilegio mínimo otorgando a tus servicios de Cloud Functions o Cloud Run solo los permisos que necesitan para acceder a los recursos requeridos. Esto minimiza el daño potencial si tu código o credenciales se ven comprometidos.
- **Análisis de seguridad:** Ranaliza periódicamente tu código, tus dependencias y tus recursos en la nube para detectar posibles exposiciones de secretos y credenciales. Estos análisis se pueden realizar con herramientas de código abierto como trufflehog y detect-secrets, o con herramientas de proveedores de nube como Sensitive Data Protection en Security Command Center.

Atacantes que utilizan la infraestructura sin servidor con fines maliciosos

En los últimos años, Mandiant ha observado que agentes de amenazas como UNC2465, UNC4713 APT41 aprovechan la infraestructura sin servidor para la distribución de malware o la comunicación de comando y control (C2). Los agentes de amenazas utilizan entornos de ejecución sin servidor como proxy para el tráfico destinado a una infraestructura controlada por el adversario o para el tráfico directamente a la máquina comprometida1. Así, los agentes de amenazas podrían ocultar su tráfico malicioso de manera más eficaz, lo que se facilita mediante las comunicaciones que se transmiten hacia y desde los subdominios del proveedor de nube.

Los agentes de amenazas tienen la capacidad de manipular funciones de tal manera que solo acepten solicitudes que cumplan con criterios específicos, como agente de usuario, rutas URI, encabezados o parámetros de consulta. En caso de que una solicitud no cumpla con uno o más de estos requisitos, los agentes de amenazas tienen la capacidad de redirigir el tráfico a un sitio web benigno o, en el caso de que se utilice una función existente, permitir que la función se ejecute como estaba previsto originalmente. El siguiente artículo de este informe amplía este tema y detalla cómo los agentes de amenazas utilizan servicios en la nube sin servidor para distribuir malware.

Mitigaciones y mejores prácticas

- Restringe el tráfico de salida de todos los recursos (en la nube y locales), excepto cuando se requiera explícitamente. Supervisa el tráfico para detectar comunicaciones con servicios en la nube no autorizados. Si se requiere una conexión saliente, el proxy web seguro de Google Cloud puede ayudar a supervisar y proteger el tráfico saliente de máquinas virtuales, contenedores y entornos sin servidor.
- Asegúrate de que las funciones y servicios sin servidor estén detrás de un API Gateway y un balanceador de carga de aplicaciones que permita beneficios de seguridad como:
  - **Integración de firewall de aplicaciones web (WAF)** para filtrar el tráfico malicioso en función de los ataques comunes en la web
  - **Integración de identidad o claves API** para controlar el acceso para autenticación y autorización
  - **Aplicación de HTTPS** para solicitudes entrantes que garantiza la implementación de cifrado en tránsito hacia y desde funciones sin servidor
  - **Registro y monitoreo mejorados** para registros detallados de llamadas API, errores, seguimiento del rendimiento de API y anomalías
- Revisa y elimina los permisos innecesarios otorgados a usuarios o roles de IAM que permiten crear, modificar o ejecutar recursos sin servidor. El recomendador de IAM puede ayudar a identificar y eliminar los permisos excesivos en Google Cloud.
- Asegúrate de que se implementen los principios de mínimo privilegio para la función o el servicio; consulta la siguiente sección para obtener orientación precisa.

Lee y entiende el diseño de seguridad de Cloud Run, que también se aplica a Cloud Functions. Ten en cuenta que ambos se ejecutan de forma predeterminada en un entorno aislado.

Arquitectura y prácticas de desarrollo inseguras

En una arquitectura sin servidor, el código se ejecuta en contenedores de corta duración. Esto significa que no hay una infraestructura persistente que atacar, lo que dificulta que los agentes de amenazas echen raíces en el entorno de la nube. Sin embargo, dado que el código en sí es el núcleo de una función sin servidor, cualquier vulnerabilidad dentro de él puede ser explotable. Esto incluye fallas de inyección (por ejemplo, inyección SQL, XSS), dependencias inseguras y errores lógicos. El riesgo es que un atacante pueda usar debilidades en los recursos sin servidor para moverse lateralmente a otra infraestructura de la nube donde pueda penetrar más profundamente o acceder a los datos.

Por ejemplo, un atacante puede aprovechar una función vulnerable para acceder a las credenciales de tu cuenta de servicio. Cloud Functions en Google Cloud utiliza una cuenta de servicio predeterminada, con rol de editor, para la ejecución de funciones. Un token de cuenta de servicio en riesgo otorga al atacante amplios permisos en todo el proyecto, incluido el de enumerar todos los depósitos de almacenamiento en la nube y recuperar los objetos que se encuentran dentro de ellos.

Mitigaciones y mejores prácticas

- **Codificación segura:** respeta los principios de codificación segura, utiliza herramientas de análisis estático y dinámico, y mantén las dependencias actualizadas para minimizar las vulnerabilidades. Además de respetar los principios, aprovecha la lista de verificación de OWASP (por ejemplo, validación de entrada, codificación de salida, manejo de errores) para obtener orientación específica. En Google Cloud, Artifact Analysis puede proporcionar información sobre vulnerabilidades para las imágenes de contenedores almacenadas en Artifact Registry.
- **Principio de privilegio mínimo:** otorga a las cargas de trabajo sin servidor solo los permisos absolutamente necesarios para su funcionamiento. En Google Cloud, recomendamos crear una cuenta de servicio única para cada recurso sin servidor y otorgarle el rol de IAM mínimo necesario. Se deben usar políticas de la organización para evitar otorgar automáticamente el rol de editor a las cuentas de servicio predeterminadas en los proyectos nuevos. Esta política ahora se aplica de forma predeterminada a todos los clientes nuevos.
- **Registro y detección:** aprovecha los registros de auditoría de la actividad del administrador para identificar el uso de la cuenta de servicio fuera de la actividad esperada. Por ejemplo, desarrolla detecciones para alertar sobre el uso de la cuenta de servicio de una función desde rangos de IP inesperados o el acceso a recursos inesperados.

Servicios de backend mal configurados

Las organizaciones que utilizan proveedores de servicios de backend sin servidor (BaaS) les confían el almacenamiento y la gestión de los datos de sus aplicaciones. Sin embargo, medidas de seguridad mal configuradas al implementar BaaS pueden exponer los datos a accesos no autorizados o filtraciones.

- **Terminales de API expuestas públicamente:** cuando se puede acceder a las terminales de API sin la autenticación o autorización adecuadas, se vuelven susceptibles de ataques. Por ejemplo, el acceso no autenticado a estas terminales permite que los atacantes investiguen vulnerabilidades, extraigan datos confidenciales y manipulen la funcionalidad de la aplicación.
- **API inseguras:** incluso con la autenticación implementada, las API pueden seguir siendo vulnerables si no cumplen con las mejores prácticas de seguridad. Por ejemplo, una validación de entrada insuficiente expone la aplicación a ataques de inyección, un manejo inadecuado de los errores puede provocar una fuga de información, y una limitación de velocidad inadecuada facilita los ataques de fuerza bruta.
- **Mala configuración:** los proveedores de BaaS ofrecen gran flexibilidad en la configuración, pero esto puede provocar, sin darse cuenta, errores de configuración que comprometan la seguridad de los datos. Por ejemplo, los controles de acceso excesivamente permisivos y las configuraciones de almacenamiento mal configuradas pueden contribuir a la exposición de los datos.

Mitigaciones y mejores prácticas

- **Automatización:** trata a las configuraciones de BaaS como código de software. Utiliza herramientas de infraestructura como código (IaC) para definir y administrar configuraciones. Esto permite controlar versiones, y probar y automatizar cambios, lo que reduce el riesgo de error humano. Antes de implementar recursos mediante IaC, utiliza una herramienta de escaneo para identificar configuraciones incorrectas y secretos.
- **Parámetros de configuración:** establece y mantén parámetros de configuración de seguridad para tu plataforma BaaS. Estos parámetros deben definir configuraciones predeterminadas seguras, controles de acceso, requisitos de cifrado y otros parámetros de seguridad.
- **Revisión de seguridad:** revisa periódicamente las configuraciones de BaaS para identificar y solucionar errores de configuración de inmediato. Las herramientas automatizadas de escaneo de configuración pueden agilizar significativamente el proceso de revisión. Estas herramientas pueden escanear las configuraciones de BaaS en busca de errores de configuración, vulnerabilidades y desviaciones de las mejores prácticas de seguridad.

Los agentes de amenazas experimentan con servicios de nube sin servidor para distribuir malware

Las arquitecturas sin servidor son atractivas para desarrolladores y empresas por su flexibilidad, rentabilidad y facilidad de uso. Estas características también hacen que sean atractivas para los agentes de amenazas, que las utilizan para distribuir y comunicarse con su malware, alojar y dirigir a los usuarios a páginas de phishing, y ejecutar malware y scripts maliciosos en entornos sin servidor. La comunidad de investigación de seguridad ha descubierto una amplia gama de abusos de la infraestructura sin servidor legítima por parte de agentes maliciosos. Este abuso afecta a todos los proveedores de servicios en la nube, incluidos Google Cloud, AWS, Azure, CloudFlare y otros.

La misión del Grupo de Análisis de Amenazas (TAG) de Google es rastrear, monitorear y contrarrestar amenazas graves contra Google y nuestros usuarios. En 2023, el TAG detectó a agentes con motivaciones económicas que abusaban de los productos Cloud Run y Cloud Functions de Google Cloud para distribuir malware y alojar páginas de phishing.

En respuesta, los equipos de Google trabajan para interrumpir el abuso mediante la búsqueda de instancias maliciosas, la actualización de las detecciones en Safe Browsing, y la incorporación de mejoras de seguridad para evitar futuras amenazas. Como se describe en el estudio de caso, nuestra intervención redujo una campaña de malware en un 99% en comparación con sus niveles máximos.

Cloud Run y Cloud Functions son servicios que ofrece Google para crear e implementar servicios web. Algunos agentes de amenazas aprovechan la flexibilidad y la facilidad de implementación de la plataforma, para garantizar que la experiencia de los usuarios sea favorable. Los paneles administrativos de la plataforma brindan información detallada sobre las solicitudes y las métricas de rendimiento. Esta es una interfaz familiar para los distribuidores de malware, ya que se parece a los sistemas de distribución de tráfico (TDS) que suelen utilizar para determinar las métricas de éxito de las campañas.

Estudios de caso

Los equipos de seguridad de Google buscan e interrumpen activamente las actividades de amenazas que intentan utilizar Google Cloud de forma subrepticia para distribuir malware. Estos estudios de casos del año pasado ilustran el enfoque proactivo de Google Cloud para detectar y contrarrestar el abuso de nuestros productos de computación sin servidor y destacan nuestros esfuerzos continuos por implementar contramedidas que mantengan protegidos a los usuarios y garanticen que nuestras plataformas sean seguras y confiables.

En ambos casos, los agentes de amenazas con motivaciones económicas utilizaron URL de contenedores y dominios legítimos de Google Cloud, como cloudfunctions.net para distribuir malware que roba información y alojar páginas de phishing de credenciales.

Distribución del ladrón de información Astaroth en Cloud Run y Cloud Functions

A lo largo de los años, los distribuidores del ladrón de información Astaroth abusaron de una amplia gama de servicios en línea y proveedores de servicios en la nube legítimos para distribuir su malware a los usuarios. Estos agentes de amenazas experimentaron con varias plataformas en la nube, incluidas Google Cloud, Amazon AWS, Microsoft Azure y otras.

Su abuso de los recursos de computación sin servidor se remonta al menos a 2019, cuando los investigadores de seguridad observaron que utilizaban Cloudflare Workers para crear URL aleatorias con el fin de evitar el análisis automatizado y entregar una carga maliciosa. Los distribuidores de Astaroth, con sede en América Latina, atacan principalmente a los usuarios de Brasil y son conocidos por su capacidad para actualizar rápidamente su malware y sus técnicas de distribución para evadir la detección.

A mediados de 2023, el TAG y Safe Browsing detectaron un abuso de Google Cloud por parte de agentes a los que rastreamos como PINEAPPLE, que aprovecharon Cloud Run y Cloud Functions para distribuir el ladrón de información Astaroth. PINEAPPLE usó instancias de Google Cloud comprometidas y proyectos de Google Cloud que ellos mismos crearon para generar URL de contenedores en dominios sin servidor legítimos de Google Cloud, como cloudfunctions.net y run.app. Las URL alojadas en páginas de destino redirigían a los objetivos a una infraestructura maliciosa que instalaba Astaroth. Si se hacía clic en ellas, las URL de Cloud Run y Cloud Function redirigían a un depósito de almacenamiento de Google Cloud que alojaba un archivo ZIP que contenía un archivo Microsoft Installer (MSI) malicioso.

PINEAPPLE intentó enviar URL maliciosas en campañas de spam mediante señuelos con temas fiscales y financieros para convencer a los usuarios de hacer clic en el enlace. La gran mayoría de estas campañas de email fueron bloqueadas al llegar a los usuarios de Gmail y Workspace. Durante un período de 14 días en junio de 2024, se bloquearon el 95% de los email. Varias de las campañas se hicieron pasar por el organismo fiscal brasileño Receita Federal do Brasil, y otras suplantaron mensajes de WhatsApp.

PINEAPPLE varió sus técnicas para convencer a los portales de correo electrónico de que sus emails eran auténticos; por ejemplo, mediante servicios de reenvío de correos, que no descartan mensajes con registros SPF fallidos, o colocando datos inesperados en el campo SMTP Return-Path para activar un tiempo de espera de solicitud de DNS y provocar fallas en las comprobaciones de autenticación de correo electrónico SPF.

Cuando detectamos que PINEAPPLE abusaba de Cloud Run y Cloud Functions, los equipos de Google trabajaron para detectar e interrumpir la actividad relacionada. Actualizamos las firmas de detección e implementamos medidas de mitigación que redujeron el volumen de las campañas de Astaroth en un 99% en comparación con el pico de la campaña.

A medida que nuestros equipos descubrieron nuevos intentos de abuso, Safe Browsing y TAG actualizaron las firmas y crearon detecciones personalizadas para identificar y bloquear las campañas. También agregamos URL maliciosas a la lista de bloqueo de Safe Browsing. Google deshabilitó los sitios maliciosos de Cloud Run y suspendió el proyecto de Google Cloud asociado. También implementamos mejoras de seguridad para aumentar significativamente la dificultad de que este agente use las plataformas.

PINEAPPLE reacciona rápidamente y adapta de forma iterativa sus tácticas, técnicas y procedimientos (TTP) en respuesta a nuevas detecciones. Después de que Google interrumpiera sus campañas de abuso a gran escala, intentaron seguir abusando de Cloud Run de forma intermitente en volúmenes más bajos.

En una campaña reciente bloqueada por Gmail, los mensajes de spam de PINEAPPLE se hacían pasar por el Ministerio de Hacienda de Brasil y dirigían a los destinatarios a una página de ingeniería social que imitaba el sistema de documentos fiscales electrónicos del gobierno brasileño (Portal da Nota Fiscal Eletrônica). El sitio dirigía a los visitantes a hacer clic en un botón para ver un documento fiscal electrónico generado por el sistema.

Si se hacía clic en el enlace, los usuarios eran redirigidos a una carga útil LNK alojada en una dirección IP controlada por el atacante. En un probable intento de evadir la detección, los atacantes incorporaron varios servicios legítimos a la campaña. Los enlaces en el sitio de ingeniería social utilizaban el protocolo ms-search:// para dirigir a los usuarios a la dirección IP de los atacantes, y los agentes de amenazas alojaron su sitio en Cloud Run de Google. Google deshabilitó el sitio malicioso de Cloud Run y suspendió el proyecto de Google Cloud asociado.

En marzo de 2024, las campañas de PINEAPPLE actualizaron temporalmente su mecanismo de distribución para usar instancias de Google Compute Engine (GCE) con direcciones IP públicas estáticas. De manera similar a su actividad anterior,

Página de ingeniería social que se hace pasar por el sistema de documentación fiscal electrónica del gobierno brasileño

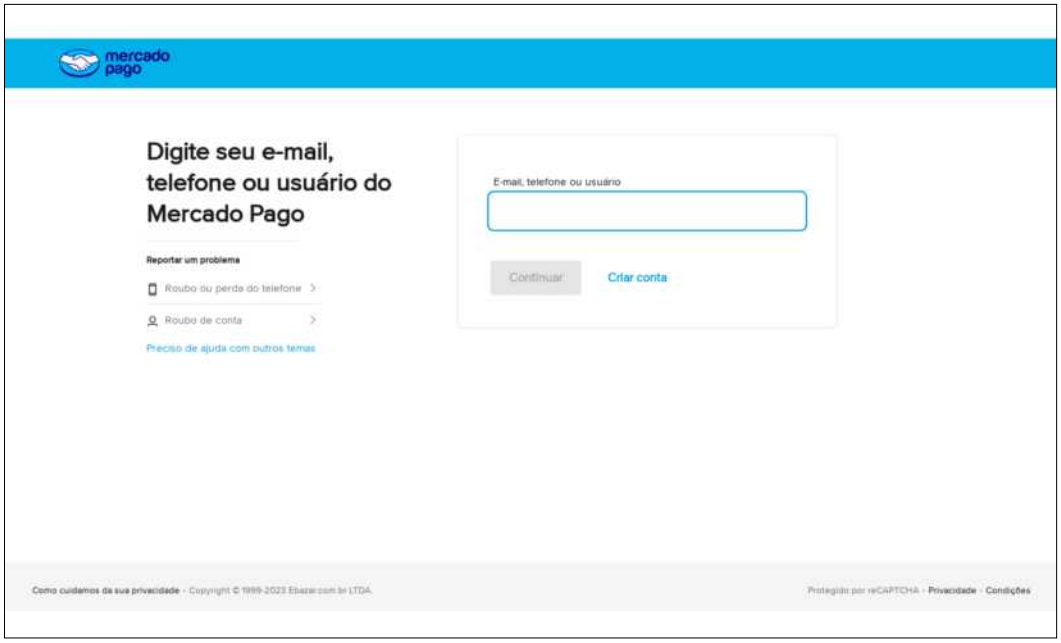
las campañas distribuían enlaces maliciosos por email. Los enlaces de GCE llevaban a un registro sin cifrar que contenía un archivo ZIP o LNK. PINEAPPLE variaba el tipo de archivo que utilizaba, incluyendo otros que no había utilizado en el pasado, como .xz y .bz2. En algunos casos, el archivo contenía archivos HTM, HTML o MSI en lugar de un LNK.

A los pocos días de intentar abusar de GCE en sus campañas, PINEAPPLE también experimentó con otras plataformas en la nube. A fines de marzo de 2024, observamos que incorporaron Azure Cloud Services y Tencent Cloud a sus campañas.

Poco después, en las campañas de mayo y junio de 2024, continuaron enviando spam que suplantaba a agencias federales brasileñas. Los email maliciosos contenían enlaces a páginas de destino en servidores virtuales dedicados creados a través del servicio de nombre de host de IP inversa de GoDaddy. Seguimos monitoreando sus campañas y actualizamos periódicamente la seguridad para garantizar que los usuarios estén protegidos.

Proyectos de phishing sin servidor

Otro agente con motivaciones financieras con sede en América Latina, FLUXROOT, experimentó con los contenedores de Google Cloud y probó las tasas de detección de las URL de Google Cloud en VirusTotal. FLUXROOT es conocido públicamente por distribuir el malware bancario Grandoreiro. En 2023, el TAG identificó varios proyectos sin servidor de Google Cloud que se utilizaban para recopilar credenciales para una de las plataformas de pago en línea más grandes de América Latina. Al descubrir los sitios de FLUXROOT, el TAG y Safe Browsing actualizaron las firmas de detección y agregaron los sitios a la lista de bloqueo de Safe Browsing.



Página de recopilación de credenciales alojada en el proyecto sin servidor de Google Cloud

Google Cloud Trust & Safety suspendió los proyectos de Google Cloud asociados y actualizó nuestras detecciones contra abusos similares. Más recientemente, FLUXROOT continuó distribuyendo el malware Grandoreiro mediante servicios en la nube como Azure y Dropbox.

Impacto

Estos estudios de casos apuntan a una preocupación creciente: el abuso de la computación sin servidor con fines maliciosos. Los agentes de amenazas aprovechan la flexibilidad y la facilidad de implementación de las plataformas sin servidor para distribuir malware y alojar páginas de phishing, y cambian sus tácticas en respuesta a las medidas de detección y mitigación de los defensores. Los agentes de amenazas de PINEAPPLE, por ejemplo, evolucionaron repetidamente sus TTP y experimentaron con diferentes servicios en la nube en sus intentos de evadir la detección y seguir distribuyendo Astaroth

Mitigaciones

Los equipos de seguridad de Google monitorean continuamente las amenazas a nuestros usuarios y los intentos de abuso de nuestros productos. Safe Browsing y el TAG actualizan periódicamente las firmas de detección y agregan dominios y URL maliciosos a la lista de bloqueo de Safe Browsing. Google Cloud Trust & Safety monitorea de manera diaria el abuso de los servicios de Google Cloud y suspende los proyectos de Google Cloud operados por atacantes, mientras que nuestro equipo de Ingeniería de Seguridad de Productos identifica brechas de seguridad y mitigaciones que ayudan a impulsar mejoras de seguridad en los productos que hacen que sea cada vez más difícil para los agentes de amenazas abusar de nuestros servicios.

También recomendamos los siguientes enfoques para ayudar a los clientes de Google Cloud a prevenir el malware en la informática sin servidor:

- Para identidades y permisos, administra de cerca las cuentas con altos privilegios y accesos de administrador, y aplica los principios de mínimo privilegio para garantizar que cada usuario tenga los permisos mínimos requeridos.
- Incorpora monitoreo y controles de Applied Threat Intelligence in Google Security Operations y Google Threat Intelligence. para detectar malware, software no deseado, exploits y otras amenazas en el host. Los protectores de la nube del sector público y privado también pueden colaborar con el Servicio de Análisis de Malware de la Agencia de Seguridad de Infraestructura y Ciberseguridad del Departamento de Seguridad Nacional de los EE. UU.
- Utiliza las alertas de Workspace para contraseñas filtradas para monitorear credenciales comprometidas, que suelen ser robadas por malware. Implementa un manual de estrategias para restablecer las credenciales de usuario y verificar los hosts afectados en busca de indicios de malware. La supervisión de amenazas digitales de Mandiant brinda protección adicional y avanzada para monitorear mercados clandestinos, sitios de pegado de datos, blogs, foros y repositorios de malware para detectar fugas de datos y credenciales desconocidas.
- Si se utiliza Cloud Run desde la perspectiva de los servicios de backend, las mitigaciones de riesgos de cargas de trabajo en contenedores incluyen la detección de amenazas de contenedores de Security Command Center de Google y abstenerse de descargar contenedores poco confiables.
- Configura los ajustes de red de Cloud Function y Cloud Run para habilitar el control de ingresos y egresos de la red hacia y desde funciones.

Colaboradores

Cris Brafman Kittner

Charles DeBeck

Kristen Dennesen

Dmitrij Lenz

Crystal Lister

Daniel Medina

Ashik Saji

Will Silverstone

Nader Zaveri

Google Cloud