Alerta

Técnica

Campañas de Phishing y robo biométrico suplantando dominios de entidades del Gobierno

COLCERT AL - 20260130 - 091

TLP:CLEAR

Resumen Ejecutivo

Se ha detectado una campaña activa de Credential Harvesting (recolección de credenciales) de alta sofisticación que suplanta la identidad de algunas entidades del Gobierno. Los atacantes emplean técnicas de ingeniería social mediante correos electrónicos diseñados para generar un sentido de urgencia, exigiendo una "validación obligatoria" de la cuenta institucional bajo la amenaza de un cierre inminente del servicio.

Detalles de la amenaza

- **Asunto del correo:** "Confirmación titularidad cuenta correo".
- **Imagen del señuelo:** La página fraudulenta imita una interfaz oficial de Microsoft Outlook. Presenta un mensaje de advertencia que indica que el inicio de sesión vencerá pronto y solicita seguir instrucciones para mantener la cuenta vigente.
- **Vector de Engaño:** El ataque redirige inicialmente a los usuarios a un sitio alojado en Google Sites para evadir filtros de seguridad: hxxps://sites[.]google[.]com/view/micrologi/p%C3%A1gina-principal.

Figura 1: Diagrama de flujo que ilustra la secuencia de ataque, desde la ingeniería social por Email hasta la obtención de credenciales por parte del atacante.

Análisis técnico e infraestructura (Para equipos de TI y Seguridad)

Se detallan los hallazgos del análisis realizado:

A. Infraestructura de alojamiento y evasión

- **Servicio de Host:** El atacante utiliza **Google Sites** (sites.google.com) para heredar la reputación de dominio de Google y evadir listas negras iniciales.
- **URL Final Analizada:** hxxps://sites[.]google[.]com/view/micrologi/p%C3%A1gina-principal.
- **IP de Servicio:** 209.85.145.113 - Google Web Servers (GWS)
- **Técnica de Evasión:** El código fuente implementa x-frame-options: DENY para evitar el análisis en entornos de sandboxing que utilicen iframes.

B. Backend de exfiltración (Punto Crítico)
A diferencia de campañas básicas, este ataque utiliza un entorno de desarrollo en la nube para procesar los datos robados, como son:

- **C2 / Exfiltration endpoint:** 6f69dfbc-3350-464e-8d20-9f23fd9993fa-00-25snioublf7id.spock.replit.dev.
- **Método:** Los datos capturados en el formulario de Google Sites son enviados vía POST hacia la instancia de **Replit** mencionada.

C. Firma del artefacto (HTML Body)

- **Hash SHA-256:** a852403abde1b208428253c4b1dfb5924e403240a727f81df1dd8d493b646552.
- **Tamaño del Body:** 95.79 KB.

Indicadores de compromiso (IoCs)

Tipo	Valor	Observación Técnica
URL de Phishing	hxxps://sites[.]google[.]com/view/micrologi/p%C3%A1gina-principal	Punto de entrada en Google Sites que suplanta a Microsoft Outlook. Bloquear la ruta específica, no el dominio raíz.
Endpoint C2 (Exfiltración)	*.spock.replit.dev	Servidor en Replit que recibe las credenciales y capturas biométricas. Es el centro de mando y control (C2) del atacante.
URL de Captura Biométrica	hxxps://6f69dfbc-3350-464e-8d20-9f23fd9993fa-00-25snioublf7id.spock.replit.dev/verificacion.html	Ruta exacta utilizada para solicitar y recibir la "selfie" de la víctima.
Hash (Payload HTML)	a852403abde1b208428253c4b1dfb5924e403240a727f81df1dd8d493b646552	Hash SHA-256 del cuerpo del sitio falso; útil para detección en sandboxes y sistemas de monitoreo de archivos.
Dirección IP (Redirección)	209[.]85[.]145[.]113	NO BLOQUEAR. IP legítima de Google Web Server (GWS) usada como fachada. Se incluye solo para análisis de correlación de tráfico.
Dirección IP (Redirección)	18[.]208[.]22[.]105 - 18[.]208[.]22[.]106 18[.]208[.]22[.]100 - 18[.]208[.]22[.]107 18[.]208[.]22[.]101 - 18[.]208[.]22[.]108 18[.]208[.]22[.]102 - 18[.]208[.]22[.]111 18[.]208[.]22[.]103 - 18[.]208[.]22[.]113	NO BLOQUEAR - Amazon Technologies Inc. Pertenecen a servicios legítimos de Trend Micro (usados a menudo como salto o proxy). Se incluye solo para análisis de correlación de tráfico.

¿Qué es replit.dev?

Replit.dev es el dominio utilizado por la plataforma **Replit** para alojar y ejecutar aplicaciones web de forma gratuita y rápida.

En el contexto del incidente, los atacantes no solo crearon una página falsa en Google Sites, sino que programaron un script (probablemente en Python o Node.js) alojado en Replit para que actúe como **C2 (Comando y Control)**. Cuando una víctima escribe su clave en el sitio falso, la información viaja directamente a la URL de replit.dev.

Nota de seguridad:

Replit no está diseñado para ser malicioso, pero como muchas plataformas legítimas (como GitHub Pages, Firebase, Netlify, etc.), puede ser abusado si no se monitorea su uso adecuadamente. Bloquear *todo* el dominio replit.dev puede generar falsos positivos, por lo que es recomendable filtrar por rutas o subdominios específicos si se detecta abuso.

Evolución crítica: Fase de captura biométrica

A diferencia de campañas convencionales, este ataque ha evolucionado para recolectar datos de identidad más profundos:

- **Solicitud de Selfie:** Una vez capturadas las credenciales, el sitio redirige a la víctima a una nueva fase titulada "Seguridad biométrica foto tipo selfie para mayor seguridad".
- **Instrucciones técnicas:** Se instruye al usuario a tomarse una foto en un espacio iluminado, con expresión neutra y sin accesorios que oculten el rostro.
- **Infraestructura de exfiltración:** Esta captura biométrica se ejecuta a través de un backend alojado en Replit: hxxps://6f69dfbc-3350-464e-8d20-9f23fd9993fa-00-25snioublf7id.spock.replit.dev/verificacion.html.
- **Persistencia:** En caso de no detectar una cámara web, el sistema lanza una alerta para forzar la verificación.

Figura 2: visualización de la captura biométrica para fraude.

Análisis de impacto adicional (biometría)

Es vital advertir sobre el uso de la **fase de captura facial**. El robo de una selfie con expresión neutra permite a los atacantes realizar:

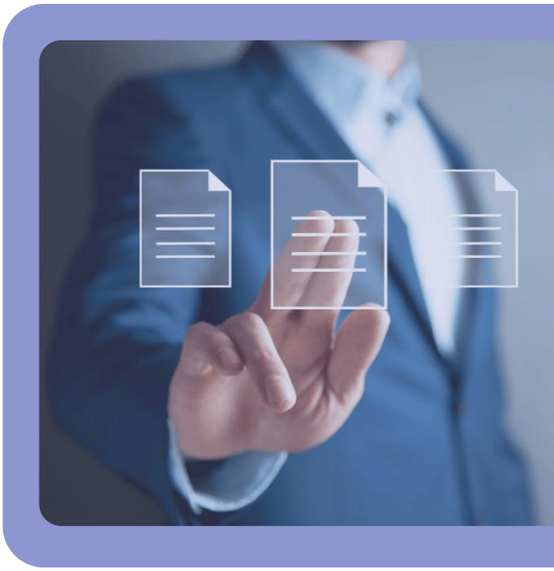
- **Bypass de KYC (Know Your Customer):** Apertura de cuentas bancarias o billeteras digitales fraudulentas que requieren validación facial.
- **Suplantación en trámites gubernamentales:** Uso de la imagen para autenticarse en portales ciudadanos que utilicen biometría como segundo factor.

Mapeo táctico mitre att&ck®

Táctica	Técnica ID	Nombre de la Técnica	Aplicación en el Incidente
Reconocimiento	T1589	Gather Victim Identity Information	**Uso de la cuenta de correo para dirigir el ataque.**
Acceso Inicial	T1566.001	Phishing: Spearphishing Attachment/Link	**Correo con asunto "Confirmación titularidad cuenta correo".**
Ejecución	T1204.001	User Execution: Malicious Link	**Requiere que el usuario haga clic en el botón "Continuar" del señuelo.**
Persistencia	T1505.003	Serverless Web App	**Uso de Replit para mantener un backend activo sin infraestructura propia.**
Evasión de Defensas	T1564.004	Steganography / Infrastructure Hijacking	**Uso de Google Sites para heredar reputación de dominio legítimo y evadir filtros.**
Exfiltración	T1567.001	Exfiltration Over Web Service	**Envío de credenciales y fotos selfie hacia el dominio replit.dev.**

Acciones recomendadas

- Filtrar el acceso al subdominio específico de Replit identificado en el análisis técnico.
- Buscar consultas hacia replit.dev desde la red institucional que coincidan con la recepción del correo de suplantación.
- Si la entidad no tiene operaciones en los países donde se alojan los servidores de Replit, recomendar el bloqueo temporal de esas zonas IP.
- Para equipos críticos o áreas administrativas sensibles, sugerir la desactivación por GPO (Group Policy Object) de la solicitud de acceso a la cámara en sitios no autorizados para evitar el éxito de la fase de Captura Biométrica.
- Recomendar la transición de MFA basado en SMS o códigos hacia llaves físicas o biometría local (Windows Hello), ya que estos métodos son resistentes al phishing de "adversario en el medio" (Adversary-in-the-Middle



Glosario técnico

- **Phishing:** Técnica de ingeniería social que utiliza correos electrónicos engañosos para suplantar a una entidad legítima (como una empresa o el gobierno). Su objetivo es manipular al usuario para que revele información confidencial, como contraseñas o datos financieros.
- **Google Sites:** Plataforma legítima de Google para la creación de sitios web.
- **SPF (Sender Policy Framework):** Lista de servidores autorizados para enviar correos en nombre de un dominio.
- **DKIM (DomainKeys Identified Mail):** Firma digital que asegura que el contenido del correo no fue alterado.
- **DMARC:** Política que indica qué hacer si SPF o DKIM fallan (Rechazar, Cuarentena o Nada).
- **Credential Harvesting (Recolección de Credenciales):** Técnica de phishing cuyo único fin es obtener nombres de usuario y contraseñas mediante formularios falsos.
- **C2 / Command & Control (Comando y Control):** Servidor o infraestructura controlada por el atacante para recibir datos exfiltrados o enviar órdenes a un malware.
- **Exfiltración de Datos:** El proceso de transferir información de manera no autorizada desde una red o sistema hacia un destino externo controlado por el atacante.
- **Sandboxing:** Entorno aislado y seguro donde se ejecuta código sospechoso para observar su comportamiento sin poner en riesgo el sistema principal.
- **Spoofing (Suplantación):** Acto de falsificar datos (como el remitente de un correo o una página web) para que parezcan provenir de una fuente confiable.

Vector de ataque : Phishing y robo biométrico

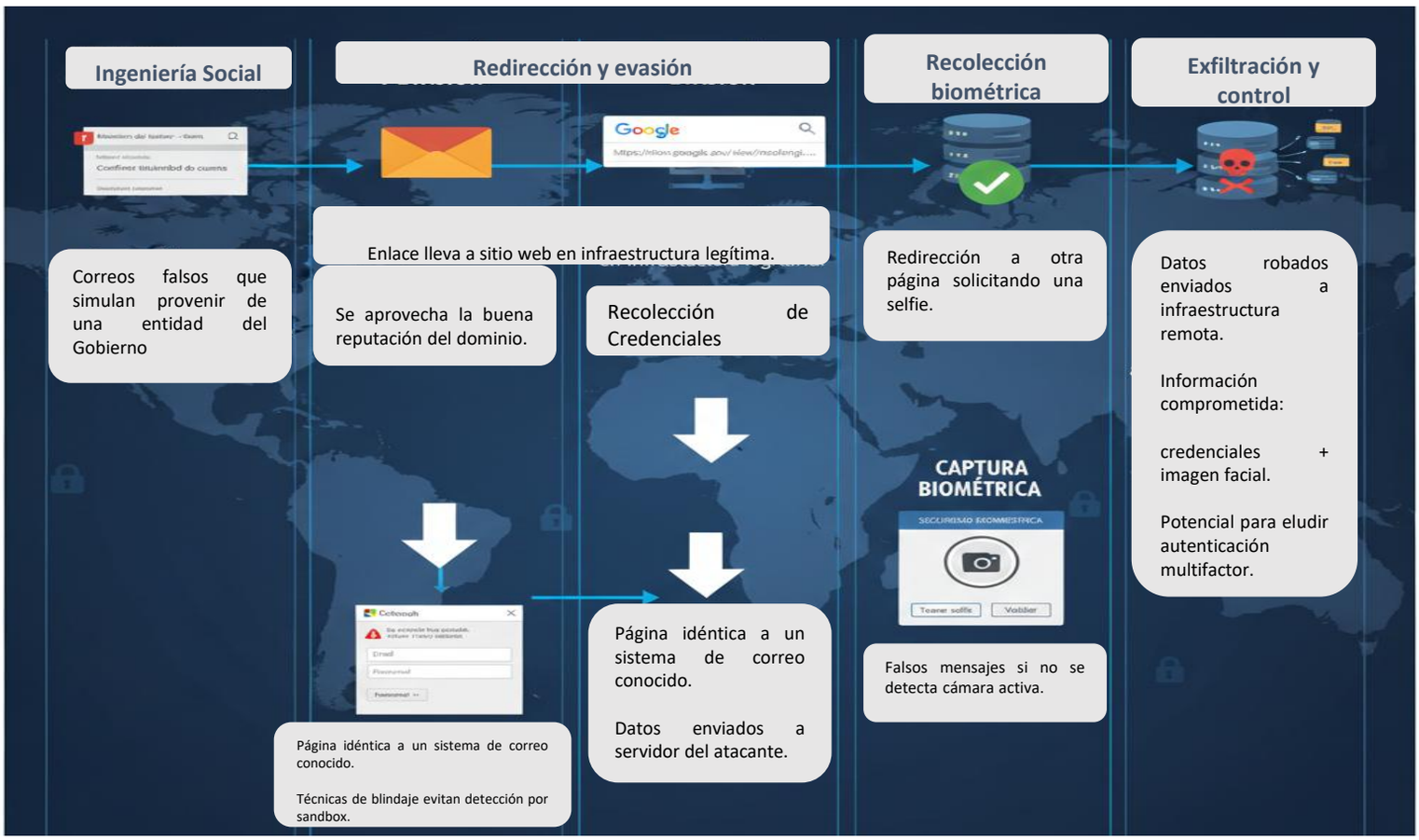


Figura 2: El diagrama describe un vector de ataque de credential harvesting altamente sofisticado que comienza con un email de engaño suplantando entidades del gobierno de Colombia bajo el asunto "Confirmación titularidad cuenta correo". La víctima es redirigida a un señuelo en Google Sites que imita una interfaz de Microsoft Outlook para robar sus credenciales, utilizando la infraestructura de Google para evadir filtros de seguridad y sistemas de sandboxing.

Posteriormente, el ataque evoluciona hacia un robo biométrico alojado en Replit, donde se solicita una "selfie" del usuario bajo el pretexto de una validación de seguridad obligatoria.

Finalmente, tanto las credenciales como la imagen facial son exfiltradas hacia un backend C2 en Replit, lo que permite a los atacantes comprometer la identidad digital del usuario y potencialmente eludir sistemas de autenticación multifactor.

Fuentes

NIST (National Institute of Standards and Technology): Referencia global para definiciones de seguridad y marcos de trabajo.

MITRE ATT&CK: Base de conocimiento sobre tácticas y técnicas de adversarios (útil para clasificar el uso de Replit como *"Serverless Computing"* o *"Web Service"*).

FIRST.org: Organización que estandariza el uso del protocolo **TLP** y la respuesta a incidentes a nivel mundial.
OWASP (Open Web Application Security Project): Guía principal para identificar y mitigar vulnerabilidades en aplicaciones web y técnicas de phishing.

ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia): Reportes de monitoreo de campañas activas en el ciberespacio nacional (Enero 2026).

Inteligencia de Amenazas Global: Referencias a tácticas TTPs (Tácticas, Técnicas y Procedimientos de Campañas de Phishing abusan Google Sites, 2026.