Alerta

Técnica

Su portal institucional podría estar siendo utilizado para promocionar sitios de apuestas ilegales

COLCERT AL – 20260212 - 094

TIC

TLP:CLEAR

Resumen Ejecutivo

El ColCERT ha identificado una campaña activa que afecta sitios web institucionales mediante la manipulación de contenidos visibles en motores de búsqueda. El ataque consiste en la inyección de contenido fraudulento —principalmente relacionado con sitios de apuestas ilegales— con el objetivo de alterar los resultados en buscadores y aprovechar la reputación del dominio afectado.

Esta modalidad opera mediante la técnica de Cloaking (Encubrimiento), en la cual el servidor entrega contenido diferenciado según quién realice la solicitud. De esta manera, muestra contenido legítimo a usuarios convencionales, mientras suministra contenido malicioso cuando detecta rastreadores de motores de búsqueda, dificultando su detección mediante navegación estándar.

- **Ciudadanos:** Ven el portal institucional legítimo.
- **Motores de Búsqueda y Navegadores:** Reciben contenido malicioso de casinos tailandeses para que este sea indexado y publicado bajo el prestigio del dominio .gov.co.

¿cómo funciona el ataque?

- **Vulnerabilidad:** El atacante entra por una falla en plugins o CMS (WordPress, Drupal) desactualizados.
- **Inyección:** Se inserta código en archivos críticos (como header.php) o en la base de datos.
- **Detección:** El servidor identifica si el visitante es un buscador.
- **Engaño:** Si es un buscador, le entrega metadatos de apuestas (títulos como 777 สล็อต y enlaces de casinos).
- **Indexación:** Google guarda esta información, y cuando alguien busca su entidad, aparecen resultados de juegos de azar.

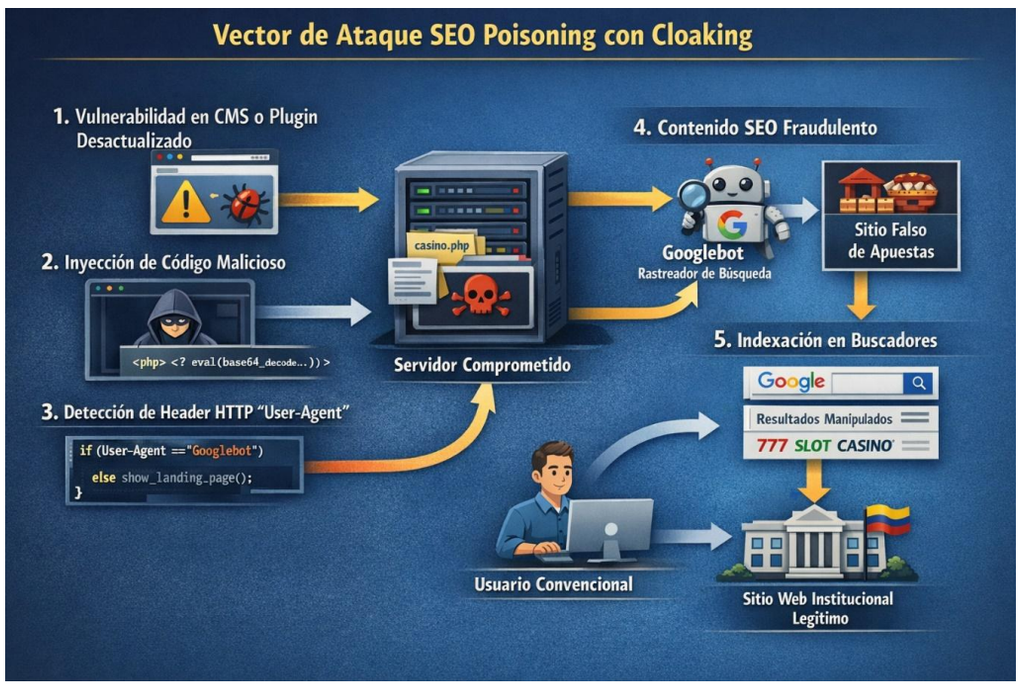


Ilustración 1 - Vector de Ataque – Manipulación de Resultados en Sitios Web Institucionales.

Indicadores de compromiso (IoCs)

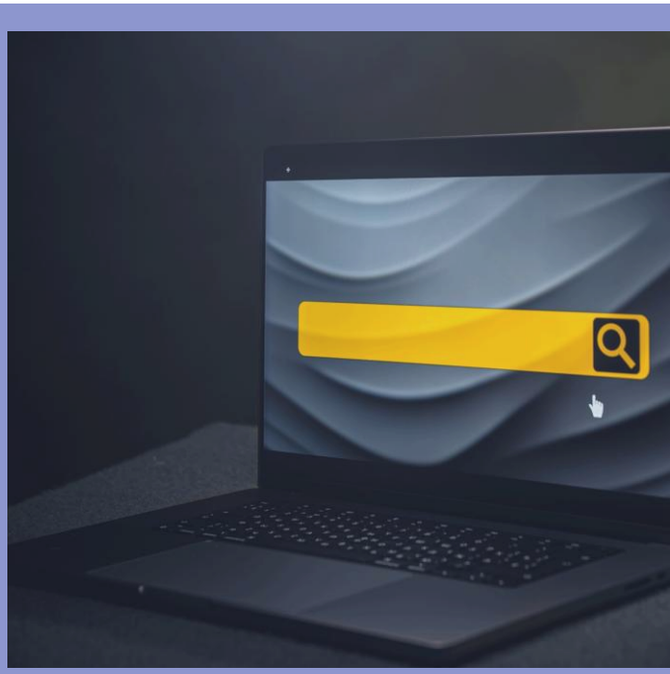
Se recomienda verificar la presencia de los siguientes indicadores técnicos asociados a campañas de manipulación SEO mediante Cloaking:

Indicadores a Nivel de Contenido Web

- Palabras clave no relacionadas con la actividad institucional: slot, casino, 777, pg slot, True Wallet, caracteres tailandeses como สล็อต.
- **Metadatos alterados:** Modificación no autorizada de etiquetas <title>, meta description, og:title, og:description.
- **Favicon externo no institucional:** Íconos que apunten a dominios externos o servicios de terceros (ej. imágenes alojadas en motores de búsqueda).
- **Enlaces ocultos en footer o plantillas:** Inclusión de hipervínculos no autorizados hacia sitios de apuestas.

Indicadores a nivel de servidor

- Archivos .php con fechas de modificación recientes o inconsistentes.
- Presencia de funciones sospechosas como:
  - eval()
  - base64_decode()
  - gzinflate()
  - shell_exec()
- Archivos con nombres similares a componentes legítimos.
- Reglas condicionales en .htaccess basadas en User-Agent.



Indicadores en motores de búsqueda

- Resultados en Google que muestren títulos distintos a los visibles al navegar.
- URLs desconocidas indexadas bajo el dominio institucional.
- Descripciones con contenido de apuestas ilegales.

La ausencia de estos indicadores no descarta compromiso, dado que la técnica de Cloaking puede activarse únicamente bajo ciertas condiciones de acceso (ej. detección específica de rastreadores).

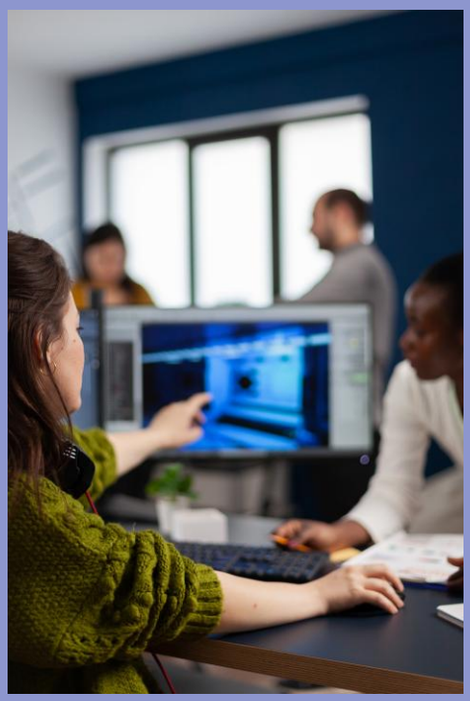
Auditoría de autogestión

Las entidades deben realizar una verificación interna inicial para identificar posible afectación:

- ❑ Ejecutar búsquedas tipo site:midominio.gov.co casino / slot / 777.
- ❑ Comparar contenido servido a usuario normal vs. simulando Googlebot.
- ❑ Revisar archivos .php con modificaciones recientes.
- ❑ Verificar cambios no autorizados en <title>, metadatos y favicon.
- ❑ Revisar .htaccess y tareas programadas (cron).
- ❑ Validar usuarios administrativos no reconocidos.

Si se detecta contenido diferencial o artefactos sospechosos, activar contención inmediata.

Acciones para equipos de TI (si se confirma compromiso)



🛑 **Contención**
- ❑ Cambiar todas las credenciales administrativas.
- ❑ Restringir accesos administrativos.
- ❑ Preservar copia de evidencia (archivos + base de datos + logs).

🧹 **Erradicación**
- ❑ Restaurar desde respaldo confiable previo al compromiso.
- ❑ Eliminar web shells y código ofuscado.
- ❑ Revisar base de datos y plantillas.

🔐 **Remediación**
- ❑ Actualizar CMS, temas y plugins.
- ❑ Implementar autenticación multifactor.
- ❑ Aplicar hardening y permisos mínimos.
- ❑ Configurar Web Application Firewall (WAF).

🌐 **Recuperación**
- ❑ Revisar Google Search Console.
- ❑ Solicitar eliminación de URLs maliciosas.
- ❑ Solicitar reindexación tras limpieza confirmada.

Recomendaciones en profundidad

- ❑ Mantener política de actualización continua.
- ❑ Implementar monitoreo de integridad de archivos.
- ❑ Bloquear ejecución PHP en directorios de carga.
- ❑ Auditar periódicamente con consultas site: en buscadores.
- ❑ Mantener registros (logs) y monitoreo continuo.

Mapeo táctico mitre att&ck

Táctica	Técnica ID	Técnica	Aplicación en el Incidente
Acceso Inicial	T1190	Exploit Public-Facing Application	Explotación de vulnerabilidades en CMS o plugins expuestos a internet, permitiendo ejecución remota de código o carga de archivos maliciosos.
Persistencia	T1505.003	Server Software Component: Web Shell	Implantación de scripts PHP maliciosos (ej. web shells tipo r57) para mantener acceso persistente y permitir reinfección.
Evasión de Defensa	T1564	Hide Artifacts	Implementación de Cloaking mediante validación del encabezado HTTP User-Agent para ocultar el contenido malicioso a administradores y mostrarlo únicamente a motores de búsqueda.
Impacto	T1491.001	Defacement: Internal Defacement	Alteración interna de títulos, metadatos, favicon y enlaces para manipulación de indexación sin modificar visiblemente la interfaz para usuarios convencionales.

Análisis técnico del encadenamiento

El comportamiento observado evidencia una cadena coherente de ataque:

- ❑ Explotación de aplicación expuesta (T1190).
- ❑ Establecimiento de persistencia mediante componente malicioso en servidor (T1505.003).
- ❑ Evasión activa mediante ocultamiento selectivo del contenido (T1564).
- ❑ Manipulación interna del contenido para afectar reputación digital (T1491.001).

El patrón corresponde a campañas automatizadas de abuso de reputación digital con persistencia y evasión activa, orientadas a manipulación SEO más que a exfiltración de información.

Se trata de un compromiso orientado a la manipulación SEO, con mecanismos de persistencia y evasión activa, sin evidencia técnica de exfiltración de información.

Glosario técnico

- ❑ **Cloaking:** Técnica donde un sitio web engaña a los buscadores mostrando contenido diferente al que ven los usuarios humanos.
- ❑ **SEO Spam:** Inyección de palabras clave y enlaces en un sitio ajeno para mejorar el ranking de portales ilegales en Google.
- ❑ **User-Agent:** Es la "identificación" que envía cualquier navegador o robot al entrar a un sitio. El atacante la usa para saber cuándo "mostrar la cara de casino" a los robots de búsqueda.
- ❑ **Payload:** Es el fragmento de código malicioso que el atacante logra insertar en su servidor para ejecutar el engaño.

Fuentes

- Investigación ColCERT: Auditoría y análisis técnico realizado en febrero de 2026.
- Google Threat Intelligence: Telemetría global de VirusTotal, Mandiant y Google Safe Browsing para la validación de reputación de infraestructura y atribución de tácticas de actores de amenaza.
- MITRE ATT&CK®: Framework internacional de tácticas, técnicas y procedimientos (TTPs) utilizado para el mapeo del comportamiento del adversario.
- FIRST (Forum of Incident Response and Security Teams): Estándares globales para la coordinación y respuesta a incidentes de ciberseguridad.