ALERTA DE SEGURIDAD DIGITAL

COLCERT AL 2204-023

REDIRECCIONES NO AUTORIZADAS: AMENAZA CRÍTICA PARA LA SEGURIDAD DIGITAL

El Centro de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT ha detectado un patrón de compromiso en varios dominios a través del análisis de fuentes abiertas. Estos dominios han sido alterados para redirigir a los usuarios hacia sitios asociados con "Robux", la moneda virtual del juego Roblox, lo cual indica la posible existencia de vulnerabilidades críticas en un espectro más amplio de dominios.

Para llevar a cabo estas acciones, los ciberatacantes emplean distintas estrategias que permiten la redirección desde sitios confiables hacia páginas con intenciones maliciosas. Entre estas estrategias se incluyen la manipulación de los sistemas de búsqueda y la inyección de código dañino en sitios web legítimos. Los métodos técnicos comunes utilizados por ciberatacantes para comprometer la seguridad en línea y redirigir a los usuarios a sitios maliciosos son variados y sofisticados, así:

Técnicas Comunes de Ciberataque organizados por criticidad

ALTO

Compromiso de sitios legítimos: Atacantes explotan fallos de seguridad en sitios web fiables para redirigir a los usuarios a páginas dañinas sin que se den cuenta.

Ataques Man-in-the-Middle, MITM: Posicionamiento del atacante en la comunicación entre el usuario y el sitio web para interceptar y alterar los datos transmitidos.

Phishing y sitios de cebo: Empleo de engaños mediante páginas que simulan ser de confianza para obtener información personal de los usuarios.

Cross-Site Scripting (XSS): Explotación de vulnerabilidades en páginas web para ejecutar scripts dañinos en el navegador y redirigir usuarios a sitios perjudiciales.

Secuestro de sesión y robo de cookies: Captura de cookies para acceder a cuentas de usuario sin autorización y realizar actividades fraudulentas.

MEDIO

Inyección de código malicioso: Incorporación de scripts o iframes en páginas web, que se activan sin el consentimiento del usuario para redirigirlo a otro sitio.

Redirecciones 301/302: Uso indebido de redirecciones legítimas para dirigir a los usuarios desde una URL original a una maliciosa sin que ellos se den cuenta.

Manipulación de resultados de búsqueda: Alteración de URL en búsquedas para redirigir usuarios a sitios controlados por atacantes, disimulados como legítimos.

SEO Poisoning (Envenenamiento SEO): El envenenamiento SEO posiciona sitios dañinos en búsquedas para atraer usuarios mediante palabras clave engañosas.

COLCERT

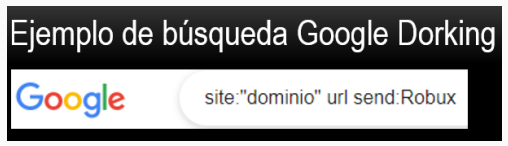
ALERTA DE SEGURIDAD DIGITAL

COLCERT AL 2204-023

REDIRECCIONES NO AUTORIZADAS: AMENAZA CRÍTICA PARA LA SEGURIDAD DIGITAL

Recomendaciones

- Realizar auditorías regulares y actualice constantemente los sistemas para mitigar vulnerabilidades. Combine esto con la gestión segura de la configuración de DNS y el desarrollo web seguro, utilizando listas blancas y cabeceras HTTP robustas.
- Implementar firewalls y sistemas de detección de intrusos para proteger contra ataques de intermediarios y realizar controles estrictos de redirecciones web y verificación de URLs para asegurar accesos seguros.
- Implemente autenticación multifactorial y administre las sesiones con cuidado, evitando el secuestro de sesión y el robo de cookies.
- Realizar pruebas de seguridad sistemáticas, como pruebas de penetración y sandboxing, para identificar y remediar inyecciones de código y otros vectores de ataque.
- Supervisar la integridad del SEO y los resultados de búsqueda para prevenir manipulaciones y ataques de envenenamiento SEO.
- Desarrollar planes de respuesta ante incidentes detallados y reporte a las instancias ciber del Estado para el apoyo y coordinación en la recuperación de las operaciones.
- Usar herramientas especializadas para detectar manipulaciones maliciosas en el código de los sitios web, identificando redirecciones no autorizadas y otros signos de compromiso. Ej: Detectic.colcert.gov.co, Sucuri SiteCheck, VirusTotal, y Google SafeBrowsing,
- Fomentar la formación continua a usuarios para identificar y reportar phishing, así como otros intentos de engaño, reforzando la seguridad con filtros de correo efectivos.



ACCIÓN URGENTE

El **COLCERT i**nvita a todas las organizaciones a informar de inmediato sobre incidentes de seguridad digital que se presenten clasificados como “Muy grave” o “Grave”, a los canales de comunicación del COLCERT, para obtener apoyo y coordinar la gestión adecuada. Por otro lado, los incidentes “Menos grave” y “Menor”, deben manejarse internamente, ejecutando protocolos de contención, erradicación y recuperación, liderados por el CISO o el responsable de seguridad digital de la organización.

Las variadas y sofisticadas tácticas de ciberataque destacan la urgente necesidad de sólidas estrategias de seguridad informática. Con amenazas cibernéticas en constante evolución, la monitorización ininterrumpida y una acción preventiva son vitales para la protección efectiva de datos y sistemas en la era digital.

FUENTES:

1.https://es.linkedin.com/pulse/inteligencia-de-fuentes-abiertas-osint-complemento-el-blanco-modelo-vdpse
2.https://www.ubilibet.com/es/3-vulnerabilidades-habituales-en-la-gestion-de-dominios/
3.https://codster.io/blog/vulnerabilidades-en-sitios-web/
4.https://es.linkedin.com/pulse/los-fallos-de-redireccionamiento-abierto-son-cada-vez-victor-ruiz
5.https://www.fastly.com/es/blog/open-redirects-real-world-abuse-and-recommendations
6.https://blog.conzultek.com/ciberseguridad/mejorar-nivel-de-ciberseguridad
7.https://es.linkedin.com/pulse/modelos-mecanismos-y-previsi%C3%B3n-antes-de-ciberataques-y-c%C3%A1ceres-meza

Como Reportar un Incidente:

https://www.colcert.gov.co/800/w3-article-198656.html