Advertencia de Seguridad

Prevención de ataques tipo Defacement

COLCERT AD-0709-021

¿Qué es el Defacement?

TLP:CLEAR

El defacement (o desfiguración) es un tipo de ataque cibernético que implica modificar la apariencia de un sitio web sin el consentimiento de su propietario. Los atacantes alteran el contenido, imágenes o enlaces, a menudo para mostrar mensajes políticos, publicitarios o de protesta. Este tipo de ataque se considera vandalismo digital y puede tener efectos perjudiciales en la reputación de las organizaciones afectadas.

Técnicas más comunes utilizadas para realizar un Defacement

Explotación de Vulnerabilidades de Software:
Los atacantes a menudo buscan y aprovechan vulnerabilidades en el software del sitio web, especialmente en sistemas de gestión de contenidos (CMS). Esto incluye la explotación de Plugins desactualizados o configuraciones incorrectas que permiten el acceso no autorizado al sistema.

Suplantación de identidad (phishing):
El phishing es una técnica común donde los atacantes envían correos electrónicos fraudulentos para engañar a los usuarios y obtener sus credenciales de acceso. Al hacerse pasar por entidades confiables, logran que las víctimas revelen información sensible que les permite acceder a los sitios y servicios web.

Inyección de código:
Los atacantes pueden inyectar código malicioso en formularios o campos vulnerables del sitio y servicios web. Esto incluye inyecciones SQL o XSS (Cross-Site Scripting), que permiten a los atacantes ejecutar scripts no autorizados o acceder a bases de datos sensibles.

Robo de Credenciales mediante Malware:
Los ciberdelincuentes pueden utilizar malware para robar credenciales de acceso. Esto puede incluir la instalación de software malicioso en el sistema de la víctima, que luego captura información sensible como nombres de usuario y contraseñas.

Ataques de fuerza bruta:
En este tipo de ataque, se utilizan herramientas automatizadas para probar múltiples combinaciones de contraseñas hasta encontrar la correcta. Este método es efectivo contra cuentas con contraseñas débiles o predecibles.

Acceso a Servidores Web Infectados:
En algunos casos, los atacantes pueden infectar directamente el servidor web con malware, lo que les permite modificar el contenido del sitio sin necesidad de acceder a él a través del CMS.

Ingeniería Social:
Los hackers pueden manipular psicológicamente a empleados o administradores para que revelen información confidencial o realicen acciones que faciliten el acceso al sistema. Este enfoque se basa en engaños y tácticas persuasivas.

Afectaciones ocasionadas

Los ataques de defacement pueden tener múltiples afectaciones para las organizaciones, sus sitios y servicios web, que van más allá de la simple alteración visual. A continuación, se detallan las principales consecuencias de estos ataques.

COLCERT

Advertencia de Seguridad

Prevención de ataques tipo Defacement

COLCERT AD-0709-021

Afectaciones Operativas

- **Indisponibilidad del sitio Web:** Tras un ataque de desfiguración, el sitio web puede volverse inaccesible o mostrar contenido no autorizado, lo que interrumpe las operaciones normales y puede afectar a los usuarios que intentan acceder a la información o servicios ofrecidos.

- **Costos de recuperación:** Las entidades de gobierno/organizaciones deben invertir tiempo y recursos significativos en restaurar el sitio a su estado original, lo que puede incluir la restauración de copias de medidas de seguridad, la reparación de vulnerabilidades y la implementación de preventivas para evitar futuros ataques.

Afectaciones reputacionales

- **Pérdida de confianza del cliente:** La presencia de contenido ofensivo o inapropiado afecta la confianza del público y los clientes en las entidades/organizaciones. Esto es especialmente crítico para entidades/empresas que manejan información sensible o que depende de su reputación en línea.

- **Impacto en la imagen corporativa:** Un ataque exitoso puede dañar gravemente la imagen pública de una entidad/empresa. Los clientes pueden cuestionar la capacidad de la entidad/organización para proteger sus datos y mantener un entorno seguro, lo que podría llevar a una disminución en las ventas o en la lealtad del cliente.

Riesgos adicionales

- **Propagación de malware:** En algunos casos, los ataques de defacement pueden ser utilizados como un medio para introducir malware en los sistemas de los usuarios que visitan el sitio comprometido, lo que amplía el impacto más allá del sitio afectado.

- **Exposición a otros ataques:** Un defacement exitoso puede indicar vulnerabilidades más profundas en la infraestructura de seguridad del sitio o servicios web. Esto puede abrir puertas en ataques adicionales más graves, como el robo de datos o ransomware.

Mejores prácticas de seguridad para evitar el Defacement:

Proteger un sitio web contra ataques de desfiguración es esencial para mantener la integridad y la reputación de una organización. A continuación, se presentan las mejores prácticas de seguridad que pueden implementarse para minimizar el riesgo de estos ataques.

Mantener actualizados todos los componentes del sitio

- **Actualización de software y complementos:** Asegúrese de que todos los complementos, temas y el software del sistema de gestión de contenido (CMS) estén actualizados. Las versiones desactualizadas pueden contener vulnerabilidades que los atacantes pueden explotar. https://www.colcert.gov.co/800/w3-article-396039.html

- **Eliminación de complementos innecesarios:** Limite la cantidad de complementos instalados y elimine aquellos que no estén en uso. Cada complemento adicional puede ser un punto de entrada potencial para los atacantes.

COLCERT

TIC

Advertencia de Seguridad

Prevención de ataques tipo Defacement

COLCERT AD-0709-021

Protección contra inyecciones SQL y XSS

Validación y saneamiento de entradas: Asegúrese de que todos los formularios y entradas de usuario estén protegidos contra inyecciones SQL y Cross-Site Scripting (XSS). Esto implica desinfectar las entradas para evitar la ejecución de código malicioso.

Utilizar HTTPS y SSL/TLS

Cifrado de datos: Habilite SSL/TLS en todas las páginas del sitio web para cifrar las comunicaciones con los usuarios. Esto ayuda a prevenir ataques como el Man in the Middle (MITM).

Implementar el principio de privilegio mínimo

Control de acceso: Limite el acceso administrativo a solo aquellos usuarios que realmente lo necesitan. Revisar y revocar privilegios innecesarios, especialmente para contratistas o colaboradores externos.

Auditorías y escaneos regulares

- **Escaneo de vulnerabilidades:** Realice auditorías periódicas y escaneos en busca de vulnerabilidades en el sitio web. Esto incluye verificar la seguridad del código fuente y buscar malware.
- **Monitoreo continuo:** Utilice herramientas automatizadas para monitorear cambios en el sitio web, lo que permite detectar rápidamente cualquier actividad sospechosa.

Capacitación continua del personal

Capacitar al personal sobre la importancia de la ciberseguridad y las mejores prácticas para gestionar plugins y otros componentes del sistema.

Gestión adecuada de archivos cargados

Restricciones en archivos cargados: Configure los permisos para que los archivos cargados por los usuarios no tengan permisos de ejecución. Además, considere realizar análisis antivirus en todos los archivos subidos.

Plan ante Incidentes

Protocolos de respuesta: Establezca un plan claro de gestión de incidentes, qué le indique que hacer en caso de un ataque exitoso, incluyendo la notificación a las autoridades pertinentes y la restauración del sitio desde copias de seguridad.

Proteger los sitios y servicios web contra el Defacement es fundamental, mantenga el CMS y sus Plugins actualizados, establezca políticas y controles de seguridad sólidos y lleve a cabo análisis de seguridad regulares para identificar y corregir vulnerabilidades, fortaleciendo así la defensa contra posibles ataques.

NIVEL DE RIESGO

ALTO

FUENTES:

- https://mineryreport.com/ciberseguridad/glosario/tipos-de-amenazas/termino/defacement/
- https://protecciondatos-lopd.com/empresas/defacement/
- https://www.incibe.es/aprendeciberseguridad/defacement
- https://www.colcert.gov.co/800/w3-article-395869.html - Guía Práctica Actualización Segura y Eficiente de Apache
- https://www.colcert.gov.co/800/w3-article-395944.html - Importancia de mantener PHP actualizado
- https://www.colcert.gov.co/800/w3-article-396039.html - Vulnerabilidades comunes de los sistemas de gestión de contenidos (CMS)

COLCERT