Reporte Incidente: Fuerza Bruta Attack 2024-05-13 #1

Globe Sistemas - Av. Libertador Jardin America

Descripción General del Reporte

Como analista de **globesistemas.com**, que presta servicios de análisis de sistemas y de ciberseguridad. Un atacante ha decidido atraer a los usuarios a un sitio web falso con malware.

La amenaza ejecutó un ataque de fuerza bruta para acceder al alojamiento web. Introdujeron repetidamente varias contraseñas predeterminadas conocidas para la cuenta administrativa hasta que acertaron con la correcta.

Una vez que obtuvieron las credenciales de inicio de sesión, pudieron acceder al panel de administración y cambiar el código fuente del sitio web. Incrustaron una función javascript en el código fuente que incitaba a los visitantes a descargar y ejecutar un archivo al visitar el sitio web. Tras integrar el programa malicioso, el atacante cambió la contraseña de la cuenta administrativa.

Cuando los clientes descargaban el archivo, eran redirigidos a una versión falsa del sitio web que contenía el malware.

Horas después del ataque, varios clientes enviaron correos electrónicos al servicio de asistencia de **globesistemas.com** Se quejaban de que el sitio web de la empresa les había incitado a descargar un archivo para acceder a su cuenta de usuario.

Los clientes afirmaron que, tras ejecutar el archivo, la dirección del sitio web cambió y sus ordenadores personales empezaron a funcionar más lentamente.

En respuesta a este incidente, el propietario del sitio web intenta acceder al panel de administración pero no lo consigue, por lo que se pone en contacto con el proveedor de alojamiento del sitio web. Todos los analistas de ciberseguridad recibimos el encargo de investigar este incidente de seguridad.

Para abordar el incidente, usted crea un entorno aislado para observar el comportamiento sospechoso del sitio web.

Ejecuta el analizador de protocolos de red tcpdump y, a continuación, teclea la URL del sitio web, **globesistemas.com**.

En cuanto se carga el sitio web, se le solicita que descargue un archivo ejecutable para actualizar su navegador. Usted acepta la descarga y permite que se ejecute el archivo. Entonces observa que su navegador le redirige a una URL diferente, **globalsistemas.com** que contiene el malware.

Los registros muestran el siguiente proceso

1. El navegador inicia una solicitud DNS: Solicita la dirección IP de la URL **globesistemas.com** al servidor DNS.
2. El DNS responde con la dirección IP correcta.
3. El navegador inicia una petición HTTP: Solicita la página web **globesistemas.com** utilizando la dirección IP enviada por el servidor DNS.
4. El navegador inicia la descarga del malware.
5. El navegador inicia una solicitud DNS para **globalsistemas.com**.
6. El servidor DNS responde con la dirección IP de **globalsistemas.com**
7. El navegador inicia una petición HTTP a la dirección IP de **globalsistemas.com**

Un analista senior confirma que el sitio web ha sido comprometido. El analista comprueba el código fuente del sitio web.

Observan que se ha añadido código javascript para incitar a los visitantes del sitio web a descargar un archivo ejecutable. El análisis del archivo descargado encontró un script que redirige los navegadores de los visitantes de **globesistemas.com a globalsistemas.com.**

El equipo de ciberseguridad informa de que el servidor web fue afectado por un ataque de fuerza bruta. El atacante descontento pudo adivinar la contraseña fácilmente porque la contraseña de administrador seguía siendo la contraseña por defecto. Además, no existían controles para evitar un ataque de fuerza bruta.

El trabajo consiste en documentar el incidente en detalle, incluyendo la identificación de los protocolos de red utilizados para establecer la conexión entre el usuario y el sitio web. También debe recomendar una acción de seguridad a tomar para prevenir ataques de fuerza bruta en el futuro.

| **Parte 1: Identificar el protocolo de red involucrado en el incidente** |
| --- |
| El protocolo implicado en el incidente es el protocolo de transferencia de hipertexto (HTTP). Dado que el problema fue con el acceso al servidor web de **globesistemas.com**, sabemos que las solicitudes de páginas web a los servidores web implican tráfico http.  Además, cuando ejecutamos tcpdump y accedimos al sitio web **globesistemas.com**, el archivo de registro de tcpdump correspondiente mostró el uso del protocolo http al contactar con el archivo . Se observa que el archivo malicioso se transporta a las computadoras de los usuarios utilizando el protocolo HTTP en la capa de aplicación. |

El objetivo principal de esta actividad fue identificar el protocolo de red utilizado en el incidente. La primera línea del informe anuncia la respuesta a ese paso.

El protocolo involucrado se determinó utilizando la información presentada en el escenario, el registro DNS y HTTP y el conocimiento que aprendió sobre el modelo TCP/IP en este curso:

* El registro de tcpdump muestra que se envía una solicitud al servidor DNS para resolver la dirección IP de la URL **globesistemas.com**. El servidor DNS responde con la dirección IP correcta. El navegador utiliza esto para dirigir a los usuarios al sitio web correcto.
* El escenario establece que cuando se carga el sitio web, una función del sitio web solicita a los usuarios que descarguen un archivo para acceder a recetas gratuitas.

Tanto el escenario como los registros indican que esta actividad ocurre a través del protocolo HTTP, que usted aprendió anteriormente que es parte de la capa de aplicación del modelo TCP/IP.

Revise el artículo "Cómo leer el registro de tráfico de tcpdump" vinculado en el Paso 2 de la actividad para obtener una explicación de la evidencia encontrada en el registro.

* Después de que el usuario descarga y ejecuta el archivo, los registros muestran que el navegador del usuario envía una nueva solicitud al servidor DNS para recuperar la dirección IP de una URL diferente: **globalsistemas.com**.

El servidor DNS envía la dirección IP al navegador de los usuarios y los usuarios son redirigidos a este nuevo sitio web a través de HTTP.

| **Parte 2: Documentar el incidente** |
| --- |
| **Resumen de los eventos y problemas identificados cuando se informó por primera vez del incidente**  Varios clientes se pusieron en contacto con el servicio de asistencia técnica del sitio web y dijeron que cuando visitaron el sitio web, se les pidió que descargarán y ejecutarán un archivo que contenía acceso a nuevas recetas.  Desde entonces, sus computadoras personales han estado funcionando lentamente. El propietario del sitio web intentó iniciar sesión en el servidor web pero notó que su cuenta estaba bloqueada.  **Descripción de las actividades de prueba involucradas en la investigación de este evento**  El analista de ciberseguridad utilizó un entorno sandbox para abrir el sitio web sin afectar la red de la empresa.  Luego, el analista ejecutó tcpdump para capturar los paquetes de tráfico de red producidos al interactuar con el sitio web.  Se le pidió al analista que descargara un archivo que afirmaba que brindaría actualización de software gratuito,, aceptó la descarga y la ejecutó. Luego, el navegador redirigió al analista a un sitio web falso **globalsistemas.com**.  **Descripción del trabajo de análisis**  El analista de ciberseguridad inspeccionó el registro tcpdump y observó que el navegador inicialmente solicitaba la dirección IP del sitio web yummyrecipesforme.com.  Una vez establecida la conexión con el sitio web a través del protocolo HTTP, el analista recordó haber descargado y ejecutado el archivo. Los registros mostraron un cambio repentino en el tráfico de la red cuando el navegador solicitó una nueva dirección IP para la URL **globalsistemas.com**.  Luego, el tráfico de la red se redirigió a la nueva dirección IP del sitio web **globalsistemas.com**.  **Conclusion del analista senior de ciberseguridad y el equipo de gestión de incidentes sobre la causa raíz del ataque**  El profesional senior de ciberseguridad analizó el código fuente de los sitios web y el archivo descargado. Descubrió que un atacante había manipulado el sitio web para agregar código que incitaba a los usuarios a descargar un archivo malicioso disfrazado de actualización del software gratuito.  Dado que el propietario del sitio web declaró que se le había bloqueado el acceso a su cuenta de administrador, el equipo cree que el atacante utilizó un ataque de fuerza bruta para acceder a la cuenta y cambiar la contraseña de administrador.  La ejecución del archivo malicioso comprometió las computadoras de los usuarios finales. |

| **Parte 3: Recomendar una solución de abordaje para ataques de fuerza bruta** |
| --- |
| Una medida de seguridad que el equipo planea implementar para protegerse contra ataques de fuerza bruta es no permitir el uso de contraseñas anteriores.  Dado que la vulnerabilidad que provocó este ataque fue la capacidad del atacante de utilizar una contraseña predeterminada para iniciar sesión, es importante que evitemos que se utilicen contraseñas antiguas, como las predeterminadas, para restablecer la contraseña.  Otra medida de apoyo es exigir contraseñas más largas. Las contraseñas de 15 caracteres o más ofrecen una mayor protección contra ataques de fuerza bruta.  Finalmente, otra solución útil es implementar la autenticación de dos factores (2FA). 2FA requiere autenticación mediante una contraseña y también confirmando un código de acceso de un solo uso (OTP) enviado a su correo electrónico o teléfono.  Una vez que el usuario confirme su identidad a través de sus credenciales de inicio de sesión y la OTP, obtendrá acceso al sistema.  Cualquier actor malicioso que intente un ataque de fuerza bruta probablemente no obtendrá acceso al sistema porque requiere autenticación adicional. |