Informe técnico – Análisis de incidente de red

Apéndice técnico: resolución de dominio malicioso

Fragmento de log capturado con tcpdump que evidencia el redireccionamiento malicioso:

14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.172 (40)

Interpretación:

- La máquina de la víctima realiza una solicitud DNS al resolver el dominio greatrecipesforme.com.
- Esta solicitud se produce justo después de ejecutar el archivo malicioso, lo que sugiere que la redirección fue generada por el malware embebido en el script JavaScript modificado.
- La respuesta del servidor DNS (en este caso Google DNS) devuelve la dirección 192.0.2.172, una IP no relacionada con el dominio original yummyrecipesforme.com.
- Conclusión: esta secuencia valida que el archivo ejecutado forzó al navegador a redirigirse a un dominio fraudulento, como parte del ataque.

Cronología forense del tráfico capturado

Hora	Evento	Descripción técnica
14:18:36	Solicitud HTTP al sitio legítimo	Se solicita la página principal de yummyrecipesforme.com vía HTTP (GET /)
14:20:32	Solicitud DNS a Google para greatrecipesforme.com	El sistema de la víctima consulta a dns.google para obtener la IP del dominio falso

14:20:32	Respuesta DNS con IP 192.0.2.172	El dominio malicioso responde con una IP no asociada al sitio legítimo
14:25:29	Inicio de conexión TCP con greatrecipesforme.com	Se establece conexión HTTP hacia el dominio malicioso

Resumen del incidente

El 23/04/2025 a las 14:20:32 , el sitio web yummyrecipesforme.com sufrió una brecha de seguridad que involucró el acceso no autorizado a la cuenta administrativa. El atacante, un exempleado, ejecutó con éxito un ataque de fuerza bruta al intentar múltiples contraseñas por defecto hasta encontrar la correcta. Esto indica que la contraseña de administrador no había sido modificada desde su configuración original.

Una vez dentro del panel de administración, el atacante modificó el código fuente del sitio web e incrustó una función JavaScript que solicitaba a los usuarios la descarga de un archivo, disfrazado como una actualización del navegador. Al ejecutar el archivo, los navegadores de los usuarios eran redirigidos automáticamente al dominio greatrecipesforme.com, el cual contenía contenido malicioso adicional.

Varias horas después de la brecha, varios clientes contactaron al equipo de soporte reportando comportamientos inusuales: aparición de mensajes para descargar archivos, redirecciones a sitios extraños y bajo rendimiento de sus equipos tras ejecutar el archivo descargado.

Para investigar el incidente, se creó un entorno aislado (sandbox) y se utilizó tcpdump para analizar el tráfico de red. Se observó la siguiente secuencia:
- El navegador realizó una solicitud DNS para yummyrecipesforme.com, que se resolvió correctamente.
- Se hizo una petición HTTP GET al sitio, y apareció el mensaje para descargar el archivo.
- Tras ejecutarlo, el navegador realizó una solicitud DNS para greatrecipesforme.com.
- La respuesta DNS devolvió la dirección IP 192.0.2.172.
- Finalmente, se estableció una conexión HTTP con el dominio malicioso.

El análisis del código fuente del sitio y del archivo ejecutado confirmó la presencia de malware responsable de la redirección. Esta conclusión fue respaldada por los registros de tcpdump, pruebas en el entorno de sandbox y los informes de usuarios.

Recomendaciones de Seguridad

Para prevenir futuros ataques de fuerza bruta, se recomienda implementar una política de bloqueo de cuenta que limite el número de intentos fallidos de inicio

de sesión.

Limitar los intentos de inicio de sesión es una medida efectiva porque impide que un atacante pueda probar un número ilimitado de combinaciones de usuario y contraseña. Al bloquear temporalmente la cuenta o requerir intervención manual tras un número definido de fallos, se frustra el uso de herramientas automatizadas y scripts maliciosos. Esta medida es sencilla de aplicar y mejora significativamente la seguridad, especialmente si se combina con contraseñas robustas y autenticación multifactor.