**Informe de incidentes de seguridad**

|  |
| --- |
| Sección 1: Identificar el protocolo de red involucrado en el incidente |
| Durante el análisis se determinó que los protocolos utilizados fueron:  **DNS** (para la resolución de dominios).  **TCP/HTTP** (para el establecimiento de conexiones y la transmisión de solicitudes GET). |
|  |

|  |
| --- |
| Sección 2: Documentar el incidente |
| En el tráfico capturado se observó que la máquina comprometida realizó consultas DNS hacia los siguientes dominios:   * **yummyrecipesforme.com → resuelto en 203.0.113.22** * **greatrecipesforme.com → resuelto en 192.0.2.17**   Posteriormente, se establecieron conexiones TCP en el puerto 80 (HTTP) y se enviaron solicitudes de tipo HTTP GET.  El patrón repetitivo de resolución DNS seguido por conexiones HTTP indica una posible actividad automatizada, común en escenarios de:   * **Phishing o redirección maliciosa de usuarios.** * **Malware con comunicación C&C (Command and Control).** * **Adware o software no autorizado que inyecta tráfico hacia dominios externos.**   El análisis en sandbox permitió corroborar que el dominio falso (greatrecipesforme.com) contiene código malicioso en JavaScript que incita a los usuarios a descargar e instalar un archivo. Este comportamiento busca robar información sensible y degrada el rendimiento de los equipos afectados.  Durante el análisis se determinó que el sitio web legítimo yummyrecipesforme.com fue vulnerado mediante un ataque de fuerza bruta contra las cuentas de administración. El uso de credenciales débiles permitió al atacante obtener acceso no autorizado a los recursos internos del sistema.  Una vez dentro, el atacante implementó un redireccionamiento malicioso desde el subdominio recetasdeliciosasparami.com hacia un sitio controlado por los atacantes (greatrecipesforme.com). El vector utilizado fue la inyección de código JavaScript malicioso, que instruía a los usuarios a descargar e instalar un archivo fraudulento.  Las pruebas realizadas en un entorno sandbox confirmaron que dicho archivo corresponde a un malware diseñado para:   * **Robar información sensible de los clientes.** * **Degradar el rendimiento de los equipos comprometidos, ocasionando lentitud y pérdida de productividad.**   Este incidente representa un ataque de tipo phishing con malware distribuido mediante inyección de código y redirección web. |

|  |
| --- |
| Sección 3: Recomendar una solución para ataques de fuerza bruta |
| Para reducir la exposición a este tipo de ataques, se recomienda implementar:   * **Políticas de filtrado DNS** para bloquear dominios maliciosos. * **Firewall de aplicaciones web (WAF)** para inspección de tráfico HTTP. * **Seguridad en endpoints (EDR/antimalware actualizado)**. * **Monitoreo continuo de tráfico** para identificar conexiones anómalas. * **Capacitación en ciberseguridad a usuarios** para reducir el riesgo de ejecución de malware. * **Autenticación multifactor (2FA)** en sistemas administrativos y políticas de contraseñas robustas. |