

SOC INCIDENT REPORT #3 – IOC Hunting (Conexiones Sospechosas)

Fecha: 17 Nov 2025

Analista: J. Rey

Severidad: Media–Alta

Estado: Abierto – Acción Requerida

Resumen:

Durante la revisión de conexiones salientes desde el host 10.0.0.5 se identificaron indicadores de compromiso (IOCs) potencialmente maliciosos, incluyendo una IP previamente asociada a intentos de fuerza bruta (203.0.113.10) y dominios sospechosos bajo el dominio evil-domain.com. El patrón sugiere posible comunicación con infraestructura de ataque (Command & Control) o servicios de verificación/actualización maliciosos.

Hallazgos:

- Tráfico saliente repetido hacia IP sospechosa: 203.0.113.10 (tres conexiones: 12:02, 12:06, 12:09).

- Dominios sospechosos detectados:

- malware-check.evil-domain.com
- suspicious-update.evil-domain.com

- Tráfico legítimo observado:

- 8.8.8.8 (Google DNS)
- 1.1.1.1 (Cloudflare DNS)
- updates.microsoft.com (actualizaciones legítimas)
- 192.168.1.1 (gateway/router local)

Análisis:

La IP 203.0.113.10 ya había sido identificada en investigaciones previas como origen de múltiples intentos de fuerza bruta contra el usuario "admin". La presencia de nuevas conexiones salientes hacia esta misma IP desde el host 10.0.0.5 incrementa fuertemente la sospecha de compromiso y posible comunicación con infraestructura de atacante.

Los dominios bajo evil-domain.com presentan patrones típicos de malware:

- "malware-check" sugiere validación del estado de infección.

- “suspicious-update” sugiere descarga de actualizaciones maliciosas o módulos adicionales.

Conclusión:

El host 10.0.0.5 muestra varios indicadores de compromiso:

- Conexiones recurrentes a IP sospechosa 203.0.113.10.
- Acceso a dominios claramente maliciosos bajo evil-domain.com.

Se recomienda tratar el host como potencialmente comprometido hasta completar una investigación forense más profunda.

Recomendaciones:

1. Aislar temporalmente el host 10.0.0.5 de la red (según política interna).
2. Bloquear la IP 203.0.113.10 y el dominio evil-domain.com (y subdominios) a nivel de firewall/proxy.
3. Ejecutar análisis antimalware y revisión forense del host (procesos, persistencia, logs adicionales).
4. Revisar otros hosts en la red en busca de conexiones hacia 203.0.113.10 o *.evil-domain.com.
5. Documentar el incidente y actualizar los playbooks de respuesta ante IOC similares.