insiderops

SEGURIDAD OFENSIVA

INFORME DE OPERACIÓN · RED TEAM

Simulación de adversario contra objetivos de negocio

Ejercicio dirigido por inteligencia, alineado con el marco TIBER-EU y con el requisito de pruebas de penetración basadas en amenazas del artículo 26 del Reglamento DORA.

DOCUMENTO DE MUESTRA · CASO FICTICIO

CLIENTE	Entidad financiera ficticia	REFERENCIA	IO-RT-0000-MUESTRA
MODALIDAD	Red team · caja negra	DURACIÓN	9 semanas
OBJETIVO	Acceso al sistema de pagos	CLASIFICACIÓN	TLP:CLEAR (muestra)
AUTOR	Mike · INSIDEROPS	VERSIÓN	1.0 · muestra pública

Reproduce la estructura y el criterio de redacción de un informe real de INSIDEROPS. Los datos, sistemas, hallazgos y organizaciones son ficticios y no corresponden a ningún cliente.

01 · PARA EL COMITÉ DE DIRECCIÓN

Resumen ejecutivo

El objetivo acordado —alcanzar la capacidad de emitir una orden de pago— se alcanzó en **diecinueve días** desde el primer contacto. La detección se produjo en el día veintitrés, cuatro días después de que un atacante real habría completado el fraude.

19	23	4
días hasta el objetivo	días hasta la primera detección	días de ventana de fraude

QUÉ OCURRIÓ, EN UNA PÁGINA

El acceso inicial no requirió explotar ninguna vulnerabilidad de software. Se obtuvo mediante una credencial de un proveedor de mantenimiento publicada por error en un repositorio de código público, válida contra el portal de acceso remoto porque ese portal no exigía segundo factor a las cuentas de proveedor.

Desde esa posición, la escalada hasta el control del dominio consumió **cuatro saltos y menos de seis horas**, aprovechando una plantilla de certificado mal configurada en la autoridad certificadora interna. Ninguno de esos cuatro saltos generó alerta.

La detección llegó cuando la operación tocó deliberadamente un servidor del entorno de pagos con una herramienta ruidosa, para comprobar si existía algún control efectivo en el último tramo. Lo había, y funcionó. El problema es que era el único.

La conclusión que importa

Su organización detecta al atacante cuando ya está dentro del entorno crítico. No lo detecta en el perímetro, ni durante la escalada, ni en el movimiento lateral. Un adversario con paciencia y sin necesidad de hacer ruido habría completado el objetivo sin ser visto.

LAS TRES DECISIONES QUE SE DERIVAN

DECISIÓN	EFECTO SOBRE ESTE EJERCICIO	PLAZO
Segundo factor obligatorio para cuentas de proveedor	Habría bloqueado el acceso inicial por completo.	30 días
Revisión de plantillas de certificado (ADCS)	Habría eliminado la ruta de escalada a administrador de dominio.	15 días
Reglas de detección en autenticación y certificados	Habría reducido la ventana de 23 días a menos de 48 horas.	90 días

El detalle técnico está en las secciones 04 y 06. Esta página se escribe para que pueda decidirse sin leer el resto.

MUESTRA

02 · MARCO DEL EJERCICIO

Alcance y reglas de enfrentamiento

Nada de lo que sigue se ejecutó sin autorización previa por escrito. Este apartado existe para que cualquier lector —incluido un auditor o un tribunal— pueda reconstruir qué estaba permitido y qué no.

OBJETIVO	Demostrar capacidad de emitir una orden de pago en tesorería, sin ejecutarla.
EN ALCANCE	Superficie expuesta, red interna, directorio activo, sedes de Madrid y Valencia, personal no directivo.
FUERA DE ALCANCE	Sistemas de terceros, banca electrónica de cliente final, comité de dirección y domicilios particulares.
VENTANA	9 semanas. Sin restricción horaria salvo en pagos, limitado a 06:00–08:00 CET.
TÉCNICAS EXCLUIDAS	Denegación de servicio, fuerza bruta masiva, corrupción de memoria en producción, cifrado o borrado de datos.
EQUIPO DE CONTROL	Tres personas designadas por el cliente. Ni el SOC ni sistemas fueron informados.
CRITERIO DE PARADA	Indisponibilidad atribuible al ejercicio, compromiso previo por un tercero, o instrucción del equipo de control.
CONTACTO 24/7	Línea directa con el operador durante toda la ventana, en ambos sentidos.

INCIDENCIAS DURANTE LA OPERACIÓN

DÍA	INCIDENCIA	RESOLUCIÓN
D+11	Evidencia de un acceso no autorizado anterior al ejercicio, ajeno al equipo ofensivo.	Escalado en 40 minutos. Ejercicio en pausa 26 horas.
D+31	Correo dirigido a una dirección fuera de alcance por un alias no documentado.	Campaña detenida y notificada el mismo día.

Sobre el hallazgo del día 11

No formaba parte del ejercicio y se comunicó de inmediato, sin esperar al informe. Por eso el procedimiento de escalado se firma antes de empezar.

MUESTRA

03 · NARRATIVA

Cronología de la operación

Cada entrada de esta tabla tiene su correspondencia en el registro de actividad completo que se entrega al equipo de defensa, con marca temporal al segundo y dirección de origen.

D+00	**Inicio de reconocimiento pasivo** Enumeración de superficie expuesta, subdominios, tecnología en uso y personal a partir de fuentes abiertas. Sin tráfico dirigido a la infraestructura del cliente.
D+06	**Credencial de proveedor localizada** Repositorio público de un integrador con un fichero de configuración que contenía usuario y contraseña de una cuenta de servicio, con el dominio del cliente en claro. Antigüedad del commit: 14 meses.
D+07	**Acceso inicial confirmado** La credencial resultó válida contra el portal de acceso remoto. La cuenta estaba exenta de segundo factor por pertenecer al grupo de proveedores.
D+09	**Reconocimiento interno** Enumeración del directorio con consultas de solo lectura, indistinguibles del tráfico legítimo de una estación de trabajo.
D+12	**Escalada a administrador de dominio** Abuso de plantilla de certificado con inscripción para clientes y nombre de solicitante arbitrario. Cuatro saltos, cinco horas y cuarenta minutos. Sin alerta.
D+15	**Persistencia y latencia** Se estableció persistencia en dos sistemas y se detuvo la actividad durante 72 horas para evaluar si algún control retrospectivo la detectaba. No ocurrió.
D+19	**Objetivo alcanzado** Acceso a la estación de operación de tesorería y demostración de capacidad de emisión de orden de pago. **No se emitió ninguna orden**: se documentó la capacidad con captura y se detuvo la acción.
D+23	**Primera detección** Un escaneo deliberadamente ruidoso sobre el segmento de pagos generó alerta en el SOC. Contención iniciada en 34 minutos, correcta y bien ejecutada.
D+24	**Revelación y cierre de la operación** Comunicación al equipo de control, entrega del registro completo de actividad y desmontaje de toda la persistencia, verificado conjuntamente.

MUESTRA

04 · ANÁLISIS

Cadena de ataque

Cinco fases encadenadas. Romper cualquiera habría hecho fracasar la operación; el interés del análisis está en identificar cuál era la más barata de romper.

01
Reconocimiento
Credencial de proveedor en repositorio público, con 14 meses de exposición.

02
Acceso inicial
Portal remoto sin segundo factor para cuentas de proveedor.

03
Escalada
Plantilla de certificado con nombre de solicitante arbitrario.

04
Movimiento
Segmentación de pagos sin control de identidad en el salto.

05
Objetivo
Capacidad de emisión de orden de pago demostrada.

COSTE DE ROMPER CADA ESLABÓN

FASE	CONTROL QUE LO HABRÍA IMPEDIDO	ESFUERZO	EFICACIA
01	Detección de secretos en repositorios públicos vinculados a proveedores	Bajo	PARCIAL
02	Segundo factor sin excepciones, incluidas cuentas de servicio y proveedor	Bajo	TOTAL
03	Revisión de plantillas de certificado y retirada del permiso de nombre arbitrario	Bajo	TOTAL
04	Autenticación fuerte en el salto al segmento de pagos	Medio	ALTA
05	Doble autorización humana para emisión de órdenes	Alto	TOTAL

Lectura recomendada. Los dos controles más baratos —fases 02 y 03— son también los de eficacia total. Romper esta cadena no exige más tecnología de detección: exige cerrar dos excepciones de configuración que la normativa interna del cliente ya recoge.

TÉCNICAS EMPLEADAS, REFERENCIADAS A MITRE ATT&CK

TÁCTICA	TÉCNICA	USO EN LA OPERACIÓN	DETECTADA
Acceso inicial	T1078.004	Cuenta válida de proveedor en servicio remoto expuesto	NO
Descubrimiento	T1087.002	Enumeración de cuentas de dominio mediante consultas LDAP	NO
Mov. lateral	T1021.002	Recursos administrativos compartidos sobre SMB	REGISTRO
Descubrimiento	T1046	Escaneo en el segmento de pagos *(ruido deliberado)*	ALERTA

MUESTRA

05 · HALLAZGO H-01

Plantilla de certificado permite suplantar a cualquier cuenta del dominio

SEVERIDAD	CRÍTICO CVSS 3.1 base 8.8 · ajustado **9.4** por alcanzabilidad confirmada
ESTADO	**Explotado y verificado**
SISTEMAS	`CA-INT-01 (autoridad certificadora) · plantilla «AccesoUsuarioVPN»`
VENTANA	D+12, entre las 09:14 y las 14:52 CET

CONDICIÓN

La plantilla `AccesoUsuarioVPN` admite inscripción por `Usuarios del dominio`, incluye autenticación de cliente y permite que el solicitante fije el nombre alternativo del sujeto. Equivale a dejar que cualquier empleado emita un carné a nombre de otro.

REPRODUCCIÓN

```
# Solicitar certificado a nombre del administrador del dominio
$ certipy req -u analista.contable@[dominio] -p [omitida] \
      -ca CA-INT-01 -template AccesoUsuarioVPN \
      -upn administrador@[dominio]
[*] Certificado guardado en administrador.pfx

# Autenticar con el certificado y obtener el hash NT
$ certipy auth -pfx administrador.pfx
[*] Nombre principal: administrador@[dominio]
[*] Hash NT obtenido [valor omitido en este informe]
```

Los valores sensibles se sustituyen por marcadores. El material completo se entrega por canal cifrado separado y se destruye de forma certificada al cierre.

IMPACTO REAL SOBRE ESTA ORGANIZACIÓN

Cualquiera de los **1.240 usuarios** del dominio puede convertirse en administrador del directorio en menos de dos minutos, sin explotar vulnerabilidad alguna y sin generar ningún evento que las reglas actuales consideren anómalo.

CORRECCIÓN

1. **Inmediata.** Retirar el permiso de nombre arbitrario, o restringir la inscripción a un grupo acotado y auditado.
2. **15 días.** Revisar el resto de plantillas: hay otras dos cercanas al mismo patrón.
3. **30 días.** Activar el registro de emisión y alertar ante certificados con nombre alternativo distinto del solicitante. Se verifica en el retest.

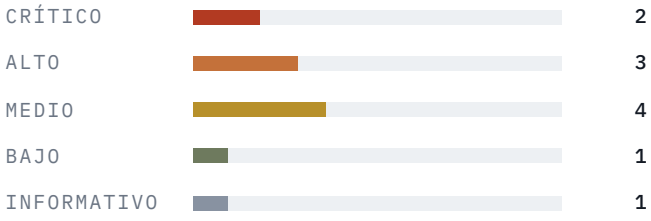
06 · INVENTARIO

Resumen de hallazgos

Once hallazgos. Cada uno se desarrolla en el cuerpo del informe con el mismo nivel de detalle que H-01: condición, reproducción, impacto sobre esta organización concreta y corrección con plazo.

REF.	SEVERIDAD	HALLAZGO	FASE	ESTADO
H-01	CRÍTICO	Plantilla de certificado permite suplantar cualquier cuenta del dominio	Escalada	Explotado
H-02	CRÍTICO	Cuentas de proveedor exentas de segundo factor en el portal remoto	Acceso	Explotado
H-03	ALTO	Credencial de servicio vigente publicada en repositorio de un integrador	Recon.	Explotado
H-04	ALTO	Salto al segmento de pagos sin verificación de identidad adicional	Lateral	Explotado
H-05	ALTO	Contraseñas en el atributo de descripción de 23 cuentas de servicio	Credenc.	Explotado
H-06	MEDIO	Delegación no restringida en dos servidores de aplicación	Escalada	Verificado
H-07	MEDIO	Retención de registros de autenticación limitada a 14 días	Detección	Verificado
H-08	MEDIO	Ausencia de alerta ante emisión anómala de certificados	Detección	Verificado
H-09	MEDIO	Estación de ingeniería con acceso simultáneo a red corporativa y de pagos	Lateral	Verificado
H-10	BAJO	Divulgación de versión en la cabecera de tres servicios expuestos	Recon.	Verificado
H-11	INFO	Metadatos de autor y ruta interna en documentos publicados en la web	Recon.	Verificado

DISTRIBUCIÓN



Once hallazgos en nueve semanas puede parecer poco frente a un informe de escáner. Cinco de ellos se explotaron de extremo a extremo; ninguno es una entrada de catálogo sin comprobar.

POR QUÉ HAY TAN POCOS

Un escáner comercial sobre el mismo alcance devolvió 312 entradas. Tras verificación manual, 41 eran reales, 19 alcanzables desde la posición de un atacante y 11 relevantes para el objetivo del ejercicio.

Lo que se entrega en este informe son esas once. Las 301 restantes están en el anexo, con el motivo de descarte de cada una, para que su equipo pueda revisar el criterio en lugar de tener que confiar en él.

MUESTRA

07 · PARA EL EQUIPO DE DEFENSA

Tabla de trazabilidad

Extracto. La tabla completa contiene 486 entradas, una por cada acción ofensiva ejecutada, y se entrega también en formato CSV para que pueda cruzarse directamente contra el SIEM.

MARCA TEMPORAL	ORIGEN	ACCIÓN	ARTEFACTO ESPERADO	RESULTADO
D+07 08:41:12	203.0.113.44	Autenticación en portal remoto con cuenta de proveedor	Evento 4624, tipo 10	SIN ALERTA
D+09 11:02:55	10.20.4.87	Consulta LDAP masiva de objetos de usuario	Evento 1644	SIN REGISTRO
D+12 09:14:07	10.20.4.87	Solicitud de certificado con nombre alternativo arbitrario	Evento 4886 / 4887	SIN ALERTA
D+12 09:16:30	10.20.4.87	Autenticación Kerberos mediante certificado	Evento 4768 con PKINIT	SIN ALERTA
D+12 14:52:19	10.20.4.87	Acceso a recurso administrativo en controlador de dominio	Evento 5140	REGISTRO
D+15 22:07:41	10.20.9.15	Creación de tarea programada con binario firmado	Evento 4698	REGISTRO
D+19 06:33:02	10.44.2.9	Sesión interactiva en estación de tesorería	Evento 4624, tipo 2	SIN ALERTA
D+23 07:11:48	10.44.2.9	Escaneo de puertos en segmento de pagos *(ruido deliberado)*	IDS · firma de barrido	ALERTA

MUESTRA

CÓMO LEER ESTA TABLA

Sin registro significa que el evento no llegó a generarse: falta configuración de auditoría. Es el caso más grave, porque no hay nada que analizar ni siquiera a posteriori.

Sin alerta significa que el evento existe y está almacenado, pero ninguna regla lo evalúa. Se corrige escribiendo la regla, no comprando producto.

Registro indica evento presente y correlacionado, sin llegar al umbral de alerta.

COBERTURA RESULTANTE

CATEGORÍA	ACCIONES	%
Sin registro	131	27
Sin alerta	268	55
Registro	72	15
Alerta	15	3
Total	**486**	**100**

El 82 % de la actividad ofensiva no llegó a evaluarse por ninguna regla. Ese porcentaje, y no el número de hallazgos, es el indicador que conviene seguir entre un ejercicio y el siguiente.

08 · PLAN

Recomendaciones priorizadas

Ordenadas por reducción de riesgo por unidad de esfuerzo, no por severidad. Las dos primeras se resuelven en una tarde y desactivan la cadena completa de este ejercicio.

#	ACCIÓN	ESFUERZO	PLAZO	HALLAZGOS
1	Retirar el permiso de nombre de solicitante arbitrario en las plantillas de certificado	Bajo	Inmediato	H-01
2	Eliminar la exención de segundo factor para cuentas de proveedor y de servicio	Bajo	30 días	H-02
3	Rotar credenciales expuestas y detectar secretos en repositorios de proveedores	Medio	30 días	H-03, H-05
4	Auditar la emisión de certificados y crear la regla de alerta	Bajo	45 días	H-08
5	Ampliar la retención de registros de autenticación a 12 meses	Medio	60 días	H-07
6	Exigir autenticación fuerte en el salto al segmento de pagos	Alto	90 días	H-04, H-09
7	Restringir la delegación en los servidores de aplicación identificados	Medio	90 días	H-06

Lo que este ejercicio no ha medido

Un red team mide una ruta, no la totalidad del riesgo. Que la operación alcanzase el objetivo por la vía descrita no significa que sea la única, y que un control resistiese aquí no garantiza que resista ante otra técnica. Este informe describe lo que ocurrió, no lo que habría ocurrido en otro escenario.

CIERRE DEL ENCARGO

SESIÓN TÉCNICA	Dos horas con sistemas y SOC, reproduciendo en directo las técnicas no detectadas.
SESIÓN DE DIRECCIÓN	Cuarenta minutos sobre el resumen ejecutivo, sin contenido técnico.
PURPLE TEAM	Jornada conjunta para escribir y validar las reglas de detección que faltan.
RETEST	Incluido, dentro de los tres meses siguientes. Verifica cada hallazgo y termina con acta de cierre.
MATERIAL	Destrucción certificada del material, con acta firmada.

MUESTRA

SOBRE ESTE DOCUMENTO

Qué es y qué no es esta muestra

Documento de muestra. Reproduce la estructura, el nivel de detalle, la maquetación y el criterio de redacción de un informe real de INSIDEROPS. La entidad, los sistemas, las direcciones, las fechas y los hallazgos son ficticios y han sido construidos para esta muestra. No corresponden a ningún cliente, real o pasado, ni reproducen ningún encargo concreto.

POR QUÉ NO VERÁ AQUÍ UN INFORME REAL ANONIMIZADO

Porque anonimizar un informe de red team es más difícil de lo que parece. La combinación de sector, tamaño, arquitectura y calendario permite identificar a una organización aunque se hayan eliminado los nombres. Publicar un informe real, aun tachado, sería incoherente con el acuerdo de confidencialidad que firmo con cada cliente antes de la primera conversación técnica.

QUÉ DEBERÍA PODER JUZGAR CON ESTA MUESTRA

- Si el resumen ejecutivo se sostiene ante un consejo sin traducción técnica intermedia.
- Si los hallazgos llevan evidencia suficiente para que su equipo pueda reproducirlos sin llamarme.
- Si la priorización responde a su exposición real o a una puntuación copiada de un catálogo.
- Si el documento distingue con claridad entre lo observado, lo inferido y lo opinado.
- Si la tabla de trazabilidad le sirve de verdad al equipo que tiene que mejorar la detección.

Si algo de lo anterior no le convence, es exactamente lo que conviene discutir antes de contratar. Los informes son el producto: si el formato no le sirve, el encargo no le va a servir.

MUESTRA

insiderops
SEGURIDAD OFENSIVA

CONTACTO	areatec@insiderops.es · Telegram @insiderops
WEB	insiderops.es
ÁMBITO	España y Unión Europea
DOCUMENTO	Muestra pública · versión 1.0 · agosto de 2026