MEMCYCO

Interrumpa los ataques antes de que se conviertan en ATO

Protección preventiva y en tiempo real frente a la suplantación de identidad y otras vías de toma de control de cuentas (ATO), mientras los ataques aún están en curso.

Anticipe la prevención de ATO

Los controles convencionales de autenticación y fraude buscan actividad sospechosa en el inicio de sesión o después del acceso.

PoSA conecta la suplantación de identidad digital y otras actividades de ataque en etapas previas con señales relacionadas con usuarios, credenciales, dispositivos, sesiones e inicios de sesión. Esto permite a las organizaciones interrumpir los ataques mientras aún están en curso, antes de que deriven en abuso de cuentas, fraude o daños a los usuarios. Además, aporta a los controles existentes un contexto más temprano para la toma de decisiones y la respuesta.

- **Reduzca las ATO exitosas, las pérdidas por fraude y el abuso de cuentas.**
- **Disminuya el volumen de incidentes, el tiempo de gestión y los costos operativos**
- **Proteja la confianza de los clientes y la experiencia digital.**
- **Fortalezca las operaciones de seguridad, la respuesta y la auditabilidad**

Múltiples vías de ATO

Diferentes vías de ataque en etapas previas pueden converger en el mismo riesgo a nivel de cuenta.



Por qué los controles existentes dejan una brecha en etapas previas

MONITOREO EXTERNO Y TAKEDOWN

Detecta y elimina activos de suplantación. Los ataques activos aún requieren protección más allá del takedown.

AUTENTICACIÓN Y CONTROL DE ACCESO

Evalúa la actividad de inicio de sesión, a menudo sin el contexto previo detrás de credenciales válidas, aprobaciones de MFA o sesiones activas.

PREVENCIÓN DEL FRAUDE

Analiza el comportamiento y la actividad de la cuenta en el inicio de sesión o después del acceso, cuando los atacantes ya pueden parecer legítimos.

LA CAPA QUE FALTA: una visión conectada desde la actividad de ataque en etapas previas hasta el riesgo a nivel de cuenta.

PoSA cierra la brecha

PoSA aporta la conexión que faltaba entre los ataques activos y el riesgo a nivel de cuenta.

Proteja durante los ataques activos
Extiende la protección más allá del monitoreo y el takedown mientras las amenazas aún están en curso.

Conecte los ataques con el riesgo de la cuenta
Correlaciona señales de suplantación, credenciales, dispositivos, sesiones e inicios de sesión en una única vista a nivel de cuenta.

Intervenga antes del fraude
Permite actuar contra accesos sospechosos antes de que deriven en fraude o abuso de cuentas.

MEMCYCO

Protección integral en todo el ciclo de vida de ATO

PoSA convierte la inteligencia sobre ataques en etapas previas en acción mediante protección e interrupción en tiempo real, al tiempo que entrega contexto de riesgo correlacionado a los sistemas y flujos de trabajo que los equipos ya utilizan.

DETECCIÓN TEMPRANA Y VISIBILIDAD CORRELACIONADA

- ✓ Detecte sitios de suplantación e infraestructura de ataque
- ✓ Identifique usuarios expuestos, credenciales comprometidas y actividad de inicio de sesión sospechosa
- ✓ Señale los dispositivos atacantes cuando se reutilizan credenciales señuelo plantadas
- ✓ Reconozca dispositivos atacantes entre sesiones, a pesar de cambios de cookies y de dirección IP

PROTECCIÓN PREVENTIVA E INTERRUPCIÓN ACTIVA

- ✓ Proteja a los usuarios mientras los intentos de ATO están en curso
- ✓ Suministre a los atacantes datos señuelo marcados en lugar de credenciales reales
- ✓ Habilite bloqueos, autenticación reforzada (step-up) o redirecciones ante actividad de inicio de sesión y de sesión de alto riesgo
- ✓ Lance campañas de engaño (deception) e inicie flujos de trabajo de takedown

CONVIERTA LA INTELIGENCIA EN ACCIÓN

- ✓ Entregue inteligencia correlacionada y lista para la toma de decisiones a los sistemas existentes en tiempo real
- ✓ Enriquezca las decisiones de inicio de sesión, fraude y riesgo de cuenta con contexto de usuario y dispositivo en tiempo real
- ✓ Conecte la actividad de ataque con los usuarios y cuentas afectados para priorizar más rápido
- ✓ Proporcione cronologías detalladas de incidentes para reducir el tiempo de investigación y gestión

Rápido de implementar. Diseñado para potenciar los controles existentes.

La integración ligera de PoSA permite obtener valor rápidamente, al tiempo que aporta a los controles existentes contexto de riesgo correlacionado que abarca todo el ciclo de vida de ATO.



IMPLEMENTACIÓN RÁPIDA Y DE BAJO ESFUERZO

Incorpore código de protección ligero en páginas web seleccionadas. El mínimo esfuerzo de integración permite un despliegue rápido. No se instala ningún software en los dispositivos de los usuarios.



POTENCIE LOS CONTROLES EXISTENTES CON PoSA

Entregue a los sistemas existentes, en tiempo real, contexto de riesgo correlacionado sobre usuarios, credenciales, dispositivos y sesiones. Detecte activos de suplantación en canales web, móviles y redes sociales, identifique accesos sospechosos y dispositivos maliciosos, y habilite acciones más tempranas para anticiparse al ATO y al fraude.

Lo que dicen los expertos del sector

"Memcyco adopta un enfoque distintivo para la prevención del phishing y de la toma de control de cuentas ... abordando un punto ciego persistente en los marcos de seguridad tradicionales."

David Mattei,
Asesor Estratégico,
Datos Insights

datos INSIGHTS

"Memcyco se infiltra en los flujos de trabajo de los ataques y actúa en múltiples puntos a lo largo del ciclo de vida del ataque. Neutraliza las amenazas antes de que escalen..."

Deepali Sathe,
Industry Principal,
Frost & Sullivan

FROST & SULLIVAN

Vea en acción la protección de PoSA contra ATO en etapas previas

Descubra cómo PoSA identifica las cuentas en riesgo e interrumpe los ataques antes de que se conviertan en tomas de control de cuentas o deriven en fraude.

Solicitar una demo

INFORME DE AMENAZAS | SECTOR DE INVERSIONES Y CORRETAJE

Cómo se detuvo una campaña de suplantación contra un bróker en un solo día de mercado

Cómo Memcyco detectó un ataque organizado contra una firma de inversiones y corretaje de Norteamérica a los 30 minutos de su lanzamiento, y detuvo al atacante dentro de las cuentas de los clientes antes de que se completara una sola orden de liquidación.

75+
dominios fraudulentos identificados
en dos meses

8+
plataformas de trading atacadas
en Norteamérica

7
cuentas de clientes protegidas
en una sola firma

US$ 2 M+
en fraude evitado
en un solo día de mercado

La amenaza

Un actor con motivación financiera, que utiliza infraestructura de hosting en Europa del Este, mantiene desde mediados de 2025 una campaña sostenida contra clientes de corretaje minorista de Estados Unidos y Canadá, que entró en una fase activa en abril de 2026. La operación es deliberada. Los dominios similares se registran con anticipación, se mantienen inactivos entre 7 y 14 días y se activan a las 9:30 a. m., con la apertura del mercado. Anuncios patrocinados en buscadores colocan el sitio falso por encima del resultado legítimo, y un acceso condicionado al anuncio deja pasar a los clientes reales mientras bloquea a los escáneres de seguridad. Un proxy de Cloudflare oculta la infraestructura real, y un dominio de reemplazo está activo dentro de las 48 horas posteriores a cada takedown.

MOTIVACIÓN
- Ganancia financiera a gran escala
- Robo de credenciales y liquidación dentro de la sesión
- Manipulación de mercado tipo pump-and-dump

SOFISTICACIÓN
- Calificada de moderada a alta
- Rotación automatizada de dominios
- Evasión de escáneres de seguridad mediante acceso condicionado a anuncios

HUELLA
- 75+ dominios en .live y .digital
- 200+ eventos de sondeo desde un mismo clúster de IP
- Activo durante las tardes de Europa del Este

Cómo funcionó el ataque y dónde lo vio Memcyco



Las credenciales ingresadas en la página de inicio de sesión falsa llegan al atacante de inmediato. Luego, el atacante inicia sesión como el cliente, liquida el portafolio y usa los fondos para comprar acciones de baja capitalización (penny stocks) que él controla, infla su precio y después las vende con ganancia. El cliente queda con un saldo en efectivo vacío y acciones sin valor, y toda la secuencia, desde la credencial robada hasta la cuenta vaciada, toma menos de cinco horas.

Un día de mercado en una sola firma



- **10:00 a. m.** Advanced Threat Detection identificó la infraestructura fraudulenta 30 minutos después de su lanzamiento, antes de que se señalara a ningún cliente, y el equipo de ciberseguridad solicitó el takedown a las 10:25 a. m.
- **11:30 a. m.** La protección en tiempo real señaló a los primeros clientes expuestos y, siete minutos después, a una víctima que llegaba desde un referido de baja reputación. La firma supo quién estaba en riesgo horas antes del ataque.
- **1:17 p. m.** El atacante ingresó a las cuentas de los clientes y comenzó a revisar las posiciones abiertas. Memcyco alertó de los inicios de sesión sospechosos en las sesiones comprometidas en tiempo real.
- **1:21 p. m.** Un analista de fraude aseguró la cuenta y bloqueó la orden de liquidación antes de que se concretara. Se protegieron siete cuentas y se evitaron más de US$ 2 M en fraude.

Por qué el takedown por sí solo no podía proteger a los clientes



El takedown se completó a las 3:35 p. m., unas seis horas después del lanzamiento. Los takedowns suelen tardar de 3 a 72 horas; este atacante necesitaba menos de cinco. Sin intervención en tiempo real, habría vaciado las cuentas comprometidas en unas cuatro horas. La protección tiene que actuar dentro de la sesión, no solo sobre el dominio.

El login es el último paso, no el ciclo de vida.

La mayoría de las firmas cree tener cubierta la suplantación de cuentas porque la detecta en el login. En esta campaña, el login llegó casi cuatro horas después de iniciado el ataque: el peor momento para empezar a buscar. Memcyco vio el ataque en su punto de formación, cuando la infraestructura se activó y los clientes quedaron expuestos, y llevó ese conocimiento hasta el momento en que apareció el atacante. **Detectar solo en el login es una apuesta. La visibilidad en todo el ciclo de vida del ataque es una estrategia.**