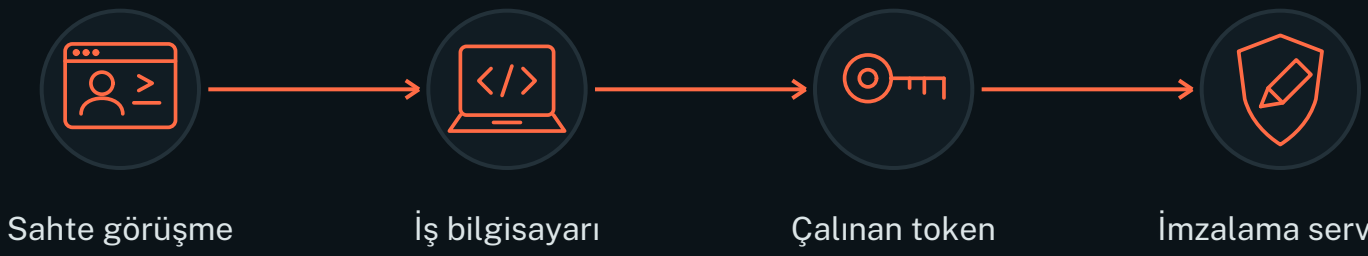
29 EKİM 2026 / SALDIRI ANALİZİ

Binance’ta ne oldu?

Geliştirici bilgisayarlarından cüzdan imzalama altyapısına uzanan yol.



$6.34B

Binance’in ilk raporuna göre etkilenen dijital varlıkların yaklaşık değeri.

Zincir nasıl ilerledi? Daha erken bir uyarı nerede üretilebilirdi?

01 / ZAMAN ÇİZELGESİ

Tek bir ihlal değildi.



HAZİRAN

Sahte araç kurulumu

A’daki sahte Homebrew kurulumu tespit edildi. Cihaz ve erişim bilgileri yenilendi.



EYLÜL

Sahte iş görüşmesi

Görüşme ödevi, B’nin iş bilgisayarında kurulum sırasında zararlı kod çalıştırdı.



20 EKİM

Şirket içi AI aracı

B üzerinden A ve C’ye erişildi. A’da deployment token’ı bulundu.



29 EKİM

İmzalama altyapısı

C’den, A’nın erişim bilgileriyle container ve zararlı script çalıştırıldı.

02 / ERİŞİMİN GENİŞLEMESİ

Bir bilgisayardan, birden fazla erişime.



03 / GELİŞTİRİCİ ARAÇLARI

Tanıdık dosya yolu. Değiştirilmiş program.

Zararlı kod, geliştiricinin kullandığı pyenv programını değiştirdi.

01 `pyenv_` — 3,414 B
Yeni dosya oluşturuldu

02 `pyenv` — 3,344 B
Meşru dosya silindi

03 `pyenv_ → pyenv` — 3,414 B
Zararlı sürüm yerini aldı

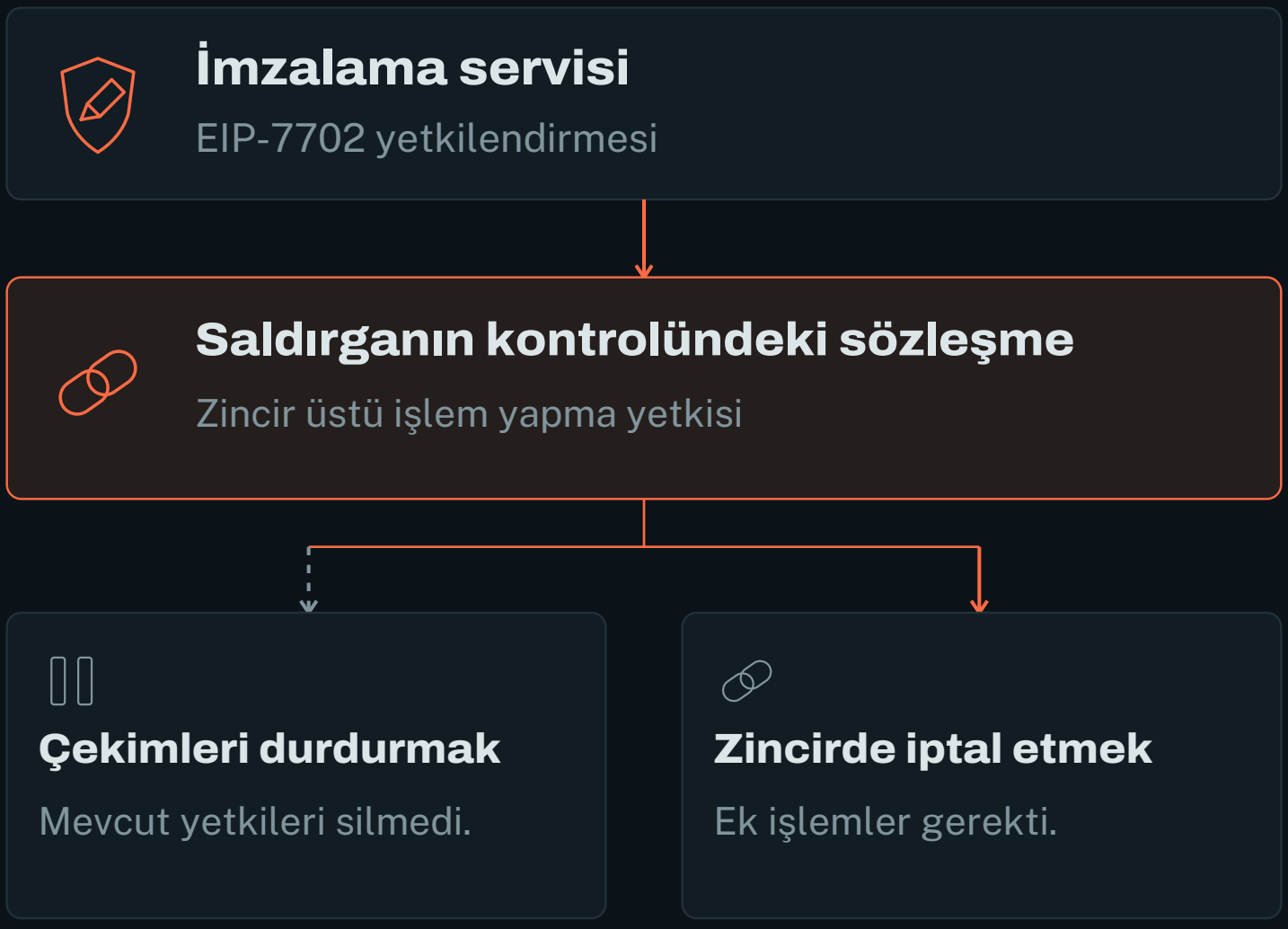
04 `symlink + zsh`
Bağlantı yeniden kuruldu; shell başlatıldı

Binance’e göre zararlı yazılım o anda endpoint korumasınca tespit edilmedi. Dosya yolu tanıdık görünüyordu.

04 / İMZALAMA VE ZİNCİR ÜSTÜ YETKİ

Çekimler durdu. Zincirdeki yetki kaldı.

Saldırgan, imzalama servisi üzerinden EIP-7702 yetkilendirmeleri oluşturdu. Bu yetkiler normal çekim akışından bağımsız çalışıyordu.



05 / DAHA ERKEN BİR SİNYAL

Erişim arayışını bir uyarıya dönüştür.

FalseTrail, saldırgan erişim bilgilerini ararken ve denerken daha erken sinyal sağlayabilirdi.



Erken sinyal, production'daki bir sonraki adımdan önce araştırma ve müdahale fırsatı yaratabilir.

06 / FALSETRAIL NASIL KATKI SAĞLAR?

Bir yem. Bir sinyal. Sonraki adımların izi.

01 YERLEŞTİR

İnandırıcı erişim bilgileri ve config'ler

Yerleşim belli; production sistemlerine gerçek yetki yok.

02 TESPİT ET

Erişim bilgisi kullanıldığında uyarı

Sinyali ekibin zaten kullandığı güvenlik araçlarına iletin.

03 GÖZLEMLE

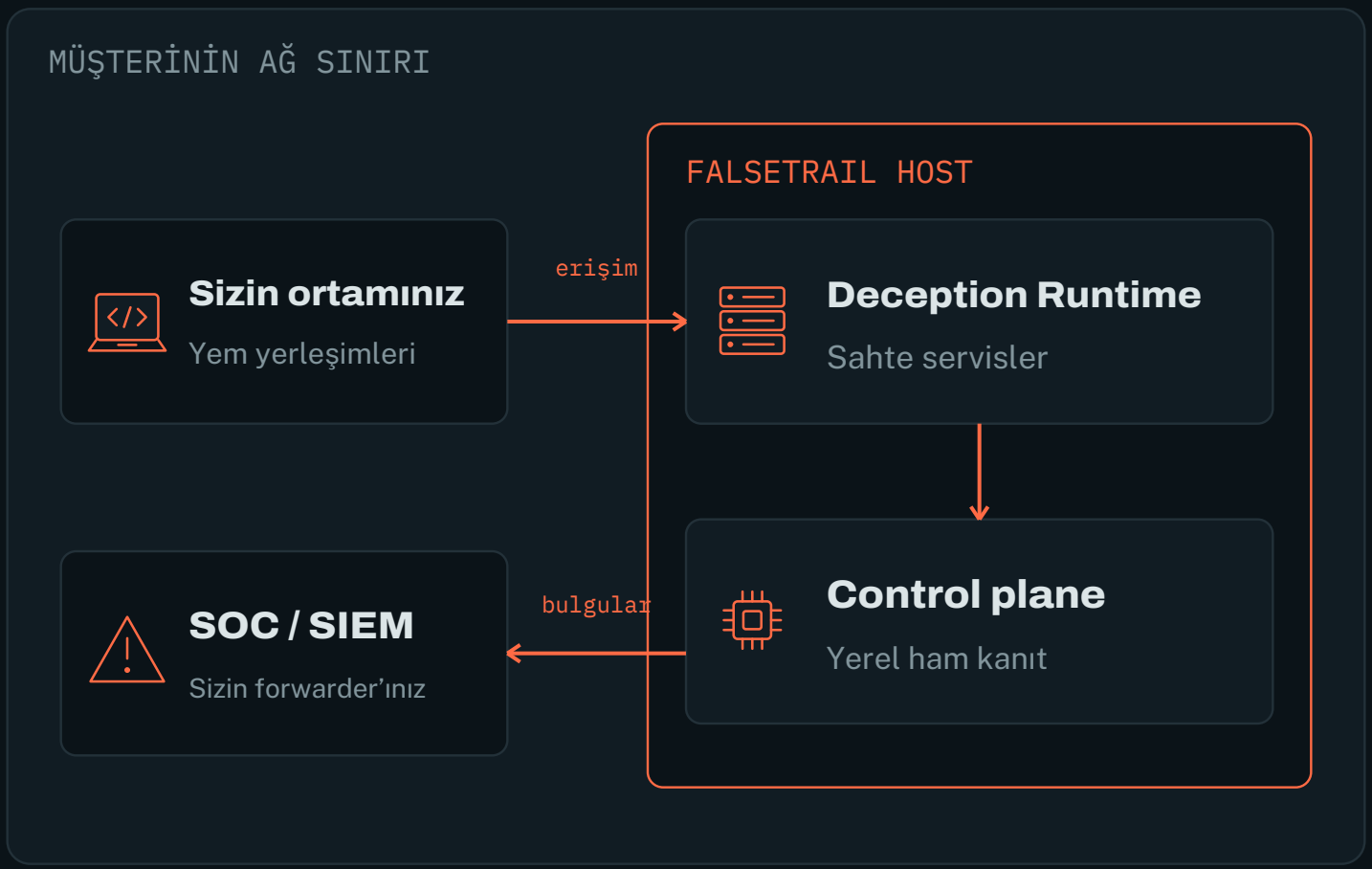
Sahte servislerde kontrollü bir iz

İz devam ederse sahte servislerdeki etkileşimleri inceleyin.

07 / SİZİN ORTAMINIZDA ÇALIŞIR

Sizin altyapınız. Sizin kanıtınız.

On-prem · Kendi bulutunuz / BYOC · Hibrit



0 **outbound connections**

Ham kanıtlar müşterinin ortamında kalır. Bulguların nereye gideceğini müşterinin forwarder'ı belirler.

08 / GÜVENLİK EKİPLERİ İÇİN

İlk girişi kaçırmak, son fırsatı kaçırmak değil.

Saldırgan zaten içeride olabilir. Yerleştirilen erişim bilgisini daha sonra kullanması, yine onu görünür kılabilir.

01

İlgi çekici yerler

Geliştirici config'lerini ve servis referanslarını, saldırganın erişim arayacağı noktalara yerleştirin.

02

Hazır bir müdahale

Uyarıyı doğrulayın. Gerçek host'u araştırın; riskli erişim bilgilerini yenileyin ve kapsamı inceleyin.

AI, daha fazla yolun daha hızlı denenmesini kolaylaştırıyor. Deception, erişim arayışından bir tespit fırsatı çıkarıyor.

09 / BİR SONRAKİ SİNYAL

Bir sonraki erişim denemesini görün.

On-prem, kendi bulutunuz/BYOC veya hibrit. Dışarı bağlantı kurmadan çalışır. Ham kanıtlar sizin ortamınızda kalır.

Ortamınız için değerlendirelim

falsetrail.com

KAYNAKLAR

Binance / Initial findings and response update
03 November 2026

FalseTrail / Deployment
Customer-hosted / zero outbound

Google / Mandiant / ARTEX and Friends
AI attack context / 30 October 2026

4 Kasım 2026 itibarıyla kamuya açık ilk bulgulara dayanan bağımsız FalseTrail analizi. Binance'in incelemesi devam ediyor. Gerçek sistemlerde araştırma ve müdahaleyi güvenlik ekibi yürütür.