29 EKİM 2026 BİNANCE SİBER SALDIRISI

Dijital Deliller, Teknik Bulgular ve Türkiye Bakımından Hukuki Sorumluluk | Kamuya Açık Kaynaklara Dayalı Uzman Değerlendirmesi

Hazırlayan: Cüneyt Üre | Adli Bilişim ve Siber Güvenlik Uzmanı

İnceleme ve kaynak kesiti: 31 Ekim 2026 | Sürüm 1.0

İNCELEMENİN NİTELİĞİ VE SINIRLARI

Bu metin, 31 Ekim 2026 tarihine kadar erişilebilir kamuya açık açıklamalar ve teknik araştırmalara dayalı bağımsız değerlendirme niteliğindedir. İlgili platformların ham sunucu günlükleri, özel anahtar yönetimi kayıtları, kullanıcı hesap defterleri veya adli imajları tarafımızca doğrudan incelenmemiştir. Bu çalışma, belirli bir dava dosyasında tarafça sunulan ve somut delil incelemesine dayanan HMK 293 uzman mütalaası yerine geçmez. Şirket beyanları, üçüncü taraf teknik bulgular ve henüz kanıtlanmamış olasılıklar birbirinden ayrılmalıdır.

Temel kaynak: Kullanıcı tarafından sunulan 31 Ekim 2026 tarihli Binance Siber Saldırısı Teknik Hukuki ve Finansal İnceleme Raporu. Aşağıdaki teknik ve hukuki değerlendirme bu raporun içeriğini koruyarak yayın düzenine aktarır.

Yönetici özeti

Olay gerçektir; ancak gönderilen görseldeki 63,3 milyar dolar rakamı, kamuya açıklanan olay tutarıyla uyumlu değildir. Binance, 29 Ekim 2026 saat 20.05 UTC civarında sıcak cüzdanlarının ele geçirilmesi sonucunda yaklaşık 6,3 milyar ABD doları değerinde varlığın kaybedildiğini bildirmiştir. TRM Labs, on blokzincirdeki ilk çıkışları işlem anındaki değerleri üzerinden yaklaşık 6,36 milyar dolar olarak hesaplamıştır. [2, 5]

Ethereum ayağına ilişkin teknik analiz, EIP-7702 işlemleriyle bir Binance sıcak cüzdanının saldırganın kontrolündeki sözleşmenin kodunu çalıştıracak şekilde yetkilendirildiğine işaret etmektedir. EIP-7702 meşru bir Ethereum standardıdır; bu olaydan Ethereum protokolünün ya da şifreleme sisteminin kırıldığı sonucu çıkmaz. TRM Labs, diğer ağlarda da geçerli imzalı transferler bulunduğunu saptamış ve imzalama altyapısına erişim ihtimalini değerlendirmiştir. Tam kök neden henüz açıklanmamıştır. [5, 6, 8]

Binance, yaklaşık 3 milyar dolarlık varlığın dondurulduğunu bildirmiştir. Dondurma, söz konusu varlıkların tamamının geri alındığı veya kullanıcı hesaplarına iade edildiği anlamına gelmez. Şirketin 31 Ekim tarihli açıklamasına göre, kaybedilen varlıkların yaklaşık %90'ına karşılık gelen tutar ilgili varlıklarla yerine konulmuş; kalan kısım için alımlar sürmüştür. Bu oran saldırgandan geri alınan varlıkların oranı değildir. [2, 3]

Binance TR, 30 Ekim'de kendi platformunda yalnızca kripto varlık çekimlerini tedbiren geçici olarak durdurduğunu, TL yatırma ve çekme ile diğer belirtilen işlemlerin sürdüğünü açıklamıştır. Bu bir şirket beyanıdır; mevcut kayıtlardan kullanıcıların tamamının bireysel durumunu doğrulamak veya Binance TR altyapısının ele geçirildiğini ileri sürmek mümkün değildir. [4]

1 İncelemenin kapsamı ve delil düzeyleri

Olay henüz adli ve teknik soruşturma aşamasındadır. Bu nedenle raporda şu ayrım uygulanmıştır: şirket beyanı, Binance veya Binance TR'nin resmî duyurusuna dayanır; zincir üstü teknik tespit, TRM Labs veya Blockaid gibi kuruluşların belirli işlemler üzerinden açıkladığı inceleme bulgusudur; istihbarat değerlendirmesi, saldırgana atıf yapılırken kullanılan teknik ve istihbari değerlendirmedir; olasılık, olayın ilerideki etkilerine ilişkin senaryo veya mesleki analizdir.

Blokzincirde bir işlemin görülmesi ile işlemi yapan gerçek kişinin kimliğinin ispatı birbirinden farklıdır. Özel güvenlik şirketlerinin yüksek güvenle ulaştığı atıflar önemlidir; buna karşılık açıklanmayan zincir dışı istihbarat bağımsız olarak sınanamadıkça bunların kapsamı sınırlıdır. Şirketlerin kendi güvenlik ürünlerine ilişkin açıklamaları da teknik bulgularından ayrı, ticari bağlamı dikkate alınarak değerlendirilmelidir.

Yüklenen Word belgesindeki bazı cümleler, soruşturma tamamlanmadan varsayımsal bir saldırı zincirini kesin olgu gibi sunmaktadır. Aynı belgedeki [1]–[7] işaretlerinin karşılığı olan bağlantılı bir kaynakça dosyada mevcut değildir. Gönderilen görselde de rakam ve teknik kavram hataları bulunduğundan, bu iki materyal bağımsız olay kanıtı olarak değil, doğrulanması gereken iddiaların listesi olarak ele alınmıştır.

2 Kronoloji

Aşağıdaki saatler, aksi belirtilmedikçe Türkiye saatiyle verilmiştir. Türkiye saati olay tarihinde UTC+3'tür. İşlem zamanlarına ilişkin ayrıntılar özellikle TRM Labs ve Blockaid değerlendirmelerine dayanır. [2, 3, 5, 6]

Burada verilen 1 Kasım tarihi bir hedef ve şirket açıklamasıdır; açıklanmış olması tek başına her ağda ve her kullanıcı için hizmetin o tarihte yeniden başladığını kanıtlamaz. 31 Ekim duyurusunda, sıfır bilgi kanıtının tamamlanması için 3 Kasım hedefi de belirtilmiştir. [3]

3 Saldırıya konu varlıkların büyüklüğü

TRM Labs'in işlem anı değerlerine göre yaptığı yaklaşık dağılım aşağıdadır. Bu, bir bilanço denetimi veya kullanıcı başına zarar tablosu değildir; kapsam, değerleme zamanı ve sonraki hareketler değiştikçe farklı kuruluşların rakamları farklılaşabilir. [5]

Ethereum satırındaki stablecoin tutarları ayrıca toplamın üzerine eklenmemelidir; bunlar zaten satırın bileşenidir. Ekran görüntüsündeki 63,3 milyar dolar, Binance'in 6,3 milyar dolar ve TRM'nin 6,36 milyar dolar açıklamasıyla uyuşmamaktadır. Ayrıca 6,36 milyar ile 6,3 milyar arasındaki fark, tek başına ilave bir hırsızlık tutarını göstermez; kullanılan değerleme ve yuvarlama yöntemleri önem taşır.

4 Merkezi borsada cüzdan ve imza mimarisi

Bir merkezi kripto varlık platformunda kullanıcıların uygulamada gördüğü bakiye çoğu zaman platformun iç hesap defterindeki alacak veya bakiye kaydıdır. Kullanıcının uygulamada bir varlığa sahip görünmesi, her kullanıcı için ayrı bir blokzincir adresinde, kendi özel anahtarıyla doğrudan kontrol ettiği aynı miktarda varlık bulunduğu anlamına gelmez. Bu durumun ayrıntısı ürün, sözleşme ve saklama modeline göre değişir.

Sıcak cüzdan, transferlerin görece hızlı işlenmesi için çevrim içi sistemlerle bağlantılı işlem ve imzalama altyapısını ifade eder. Soğuk saklama ise özel anahtarın veya imzalama sürecinin sürekli çevrim içi ortamdan ayrılması esasına dayanır. Anahtarın saklandığı donanım, kullanılan HSM veya MPC düzeni ve imza politikası, yalnızca cüzdanın sıcak ya da soğuk diye adlandırılmasından daha açıklayıcıdır.

Tipik bir çekim akışında kullanıcı talebi alınır; hesap, risk ve uyum kontrolleri yapılır; cüzdan hizmeti işlem hazırlar; ayrı bir imza bileşeni koşullar sağlanırsa işlemi imzalar ve işlem ağa gönderilir. İyi tasarlanmış bir

mimaride talebi oluşturan sistemin işlemi tek başına imzalatabilmesi beklenmez; limitler, bağımsız onaylar, hedef adres kuralları ve anahtar korumaları birbirini tamamlar. Somut olayda bu kontrollerin fiilen nasıl yapılandırıldığı ise henüz kamuya açık tam bir kök neden raporuyla doğrulanmış değildir.

5 İlk erişim hakkında bilinenler ve bilinmeyenler

Binance'in ilk açıklamasına göre olay, bir DevOps mühendisinin ele geçirilmiş olabilecek dizüstü bilgisayarıyla bağlantılı olabilir; bu durum bir servis konteynerine erişim ve yetkisiz çekim işlemleri gönderilmesini mümkün kılmış olabilir. Şirket sonraki açıklamasında ek ihlal noktaları bulunduğunu ve incelemenin devam ettiğini belirtmiştir. Bu sebeple “tek bir mühendis bütün borsayı çökertti” veya “tek aşamalı bir parola hırsızlığı yaşandı” denilemez. [1, 2]

Servis konteyneri, bir uygulamanın ve bağımlılıklarının izole edilerek çalıştırıldığı yazılım ortamıdır. Ancak konteynere girildiğinin söylenmesi, saldırganın mutlaka kriptografik anahtarları dosya olarak kopyaladığı anlamına gelmez. Ortamda çalışan bir servisin yetkisini, servis hesabını, oturum belirtecini veya işlem oluşturma arayüzünü kötüye kullanmak teorik olarak mümkündür. Bunlar genel senaryolardır; hangisinin bu olayda gerçekleştiği açıklanmış değildir.

Erişim yolu; oltalama, zararlı yazılım, yazılım tedarik zinciri, ele geçirilmiş kimlik bilgisi veya başka bir yöntem olabilir. Bu olasılıkların her birinin somut olaya uygulanması için uç nokta imajları, kimlik ve erişim kayıtları, süreç ağaçları, ağ bağlantıları, konteyner günlükleri ve ilgili zaman çizelgeleri gerekir. Yüklenen belgede geçen sıfırıncı gün açığı, belirli zararlı yazılım türü ve kesin yanal hareket iddiaları, bu kaynaklarla doğrulanmış olay bulgusu olarak yazılmamalıdır.

Binance, şu aşamada cüzdan özel anahtarlarının sızdırıldığına ilişkin kanıt bulmadığını söylemiştir. Bu açıklama, yetkisiz imzaların üretilmediği anlamına gelmez: saldırgan korumalı bir anahtarı dışarı çıkarmadan, anahtarı kullanan meşru imzalama servisinin yetkisini istismar etmiş olabilir. Tam tersine, kamuya açıklanmamış başka bir anahtar ihlali ihtimali de yalnızca bu beyanla kesin biçimde dışlanamaz. [1, 2, 5]

6 EIP 7702 yetkilendirmesinin teknik analizi

6.1 Standart ne işe yarar

EIP-7702, Ethereum'da bir dış hesap adresinin, yetkilendirme imzası aracılığıyla belirli bir akıllı sözleşmenin koduna işaret etmesini sağlayan standarttır. Böylece toplu işlemler, farklı ücret ödeme düzenleri ve programlanabilir hesap davranışları gibi meşru kullanım alanları ortaya çıkar. Standart, Ethereum'un Pectra güncellemesiyle 2025'te devreye girmiştir. [5, 8]

Teknik yapıda işlem tipi 0x04 olan bir işlem, bir veya daha fazla yetkilendirme kaydı taşıyabilir. Her yetkilendirme kaydı zincir kimliği, devredilen kod adresi, ilgili hesabın nonce değeri ve imza bileşenlerini içerir. Başarıyla işlenen kaydın ardından hesaba sözleşme kodunu işaret eden 0xef0100 önekiyle bir gösterge yazılır. Sözleşme kodu ilgili hesap bağlamında yürütüldüğünden, kodun neyi mümkün kıldığı varlık güvenliği açısından belirleyicidir. [8]

Yetkilendirmenin varlığı, özel anahtarın saldırganın cihazına kopyalandığını tek başına ispatlamaz. Aynı derecede önemli olan husus, geçerli imzanın kimin hangi kontrol süreci üzerinden ürettirildiğidir.

6.2 Elli yetkilendirme ve nonce penceresi

Nonce, hesapla ilişkili sıralama ve tekrar kullanımını önleme işlevi gören sayaçtır. Aktif bir borsa cüzdanının sayacı, normal işlemler devam ederken değişebilir. Blockaid'e göre saldırgan, Binance 14 olarak etiketlenen sıcak cüzdan için 18.914.775 ile 18.914.824 arasındaki 50 farklı nonce değerine karşılık gelen yetkilendirmeleri aynı tür-4 işlemine dahil etmiştir. En az bir yetkilendirme, işlem işlendiğinde geçerli koşullarla eşleşmiş ve cüzdan saldırganın sözleşmesine yönlendirilmiştir. Bu mekanizma, hareketli bir sayaca karşı farklı olası değerlerin önceden hazırlanması şeklinde anlaşılabilir. [6]

Burada saldırganın 50 ayrı kullanıcının hesabını ele geçirdiği, 50 özel anahtar çaldığı veya 50 blockchain ağında işlem yaptığı sonucu çıkmaz. Söz konusu sayı, bir cüzdanla ilişkilendirilen yetkilendirme kayıtlarının sayısıdır.

6.3 Süpürme sözleşmesi ve ilk büyük transfer

Blockaid'in incelemesine göre yetkilendirilen sözleşme, yalnızca saldırganla ilişkilendirilen operatörün çağrısına izin veren ve varlıkları belirli hedefe aktaran bir kod içeriyordu. Zincir üstü yetkilendirmeden 3 dakika 24 saniye sonra operatör bu mekanizmayı kullanarak yaklaşık 167.464 ETH, 1,615 milyar USDT ve çok sayıda başka tokenı bir toplama adresine yönlendirdi. Blockaid, bu ilk sepetin olay anı değerini yaklaşık 2,5 milyar dolar olarak hesapladı. Bu tutar, toplam olay büyüklüğünün bir parçasıdır; 6,3 milyarın üzerine eklenmez. [6]

Yetkilendirmenin devam etmesi, sonradan aynı adrese gelen varlıkların da yeni bir yetkilendirme imzasına gerek olmadan sözleşmenin izin verdiği ölçüde risk altında kalmasına neden olabilir. Blockaid, daha sonra cüzdana gelen varlıkların da alındığını ve ilişkili bir akıllı hesaptan USDC transfer edildiğini raporlamıştır. Bu tespit, olay müdahalesinde yalnızca ilk çıkışın izlenmesinin yeterli olmadığını gösterir. [6]

6.4 Yetkilendirme nasıl sınırlandırılır

EIP-7702 standart metni, hesabın yetkilendirme işaretinin yeni bir geçerli yetkilendirme ile değiştirilmesini veya sıfır adresi kullanılarak temizlenmesini öngörür. Ancak olayın sürmesi sırasında bu işlemin, mevcut erişim ve diğer riskler değerlendirilerek profesyonelce yapılması gerekir. Yeni bir adrese geçmek eski adresteki yetkilendirmeyi kendi kendine silmez; buna karşılık saldırgan eski hesabı kontrol ediyorsa yalnızca yetkiyi kaldırma girişimi de tek başına her durumda yeterli koruma sağlamaz. [8]

Borsa yönünden temel koruma, imza üretilmeden önce istenmeyen EIP-7702 yetkilendirmelerini reddeden bağımsız politika, yalnızca onaylı akıllı sözleşmelere izin verilmesi, imzaların anlamsal içeriğinin gösterilmesi ve cüzdanın kod durumundaki değişikliklerin izlenmesidir. Blockaid bu alanda kendi ticari ürününü önermektedir; önerinin geçerliliği ürün adından bağımsız olarak test edilebilir kontrol gereksinimleriyle değerlendirilmelidir. [6]

7 Diğer ağlardaki transferler ve teknik sınırlar

TRM'ye göre Ethereum dışındaki çeşitli ağlarda da Binance ile ilişkilendirilen cüzdanlardan saldırganın kontrol ettiği değerlendirilen adreslere olağan biçimde imzalanmış transferler yapılmıştır. Bitcoin, XRP Ledger, Tron ve Solana gibi ağların hepsinde Ethereum'un EIP-7702 standardı işletilmez. Dolayısıyla “on blokzincirin tamamı EIP-7702 açığıyla hacklendi” ifadesi teknik olarak yanlıştır. [5]

TRM, farklı anahtar tipleri ve imza düzenleri kullanan ağlarda kısa süre içinde geçerli transferler görülmesini, ortak veya bağlantılı bir imzalama altyapısının kötüye kullanılmış olabileceğine ilişkin kuvvetli bir gösterge olarak değerlendirmiştir. Bu teknik çıkarım, şirketin nihai adli inceleme raporuyla doğrulanmış

tam kök nedenin yerine geçmez. Hangi servis hesabının, hangi onay aşamasının ve hangi anahtar saklama düzeninin nasıl etkilendiği ayrıca araştırılmalıdır.

Bu saldırıdan “Bitcoin zinciri kırıldı”, “Ethereum madencileri/validatörleri sistemi hackledi” veya “tüm kullanıcıların bireysel anahtarları çalındı” sonucu da çıkmaz. Eldeki bulgular, öncelikle borsanın kontrol ettiği cüzdan ve işlem yetkilendirme süreçleri üzerinde yoğunlaşmaktadır.

8 Fail atfı ve Kuzey Kore iddiası

TRM Labs, saldırıyı zincir üstü ve zincir dışı istihbarata dayanarak yüksek güven düzeyiyle Kuzey Kore bağlantılı TraderTraitor grubuna atfetmiştir. Kullanılan hazırlık adımları, operatör cüzdanının finansmanı ve önceki saldırılarla gösterilen benzerlikler gerekçe olarak ileri sürülmektedir. Bu, ciddi bir uzman kuruluş değerlendirmesidir; ancak açıklanmayan zincir dışı veriler bağımsız olarak değerlendirilememektedir. [5]

FBI, 2025 yılındaki yaklaşık 1,5 milyar dolarlık Bybit saldırısını TraderTraitor faaliyetine atfetmiştir. Ne var ki önceki bir olay hakkında yapılan resmî atıf, 2026 Binance olayındaki sorumluluğu otomatik olarak kanıtlamaz. Her olayın kendi delilleri ayrıca incelenmelidir. Bu raporun eriştiği kaynaklarda Binance olayına ilişkin kesinleşmiş yargı kararı veya bireysel fail kimliğinin bağımsız biçimde doğrulandığı bir adli sonuç bulunmamaktadır. [20]

Faile ilişkin kimliklendirmede adres kümeleri, takas veya borsa kayıtları, hesap açılış verileri, sunucu ve erişim günlükleri, ele geçirilen cihaz delilleri, uluslararası adli yardımlaşma yanıtları ve olayla ilişkilendirilmiş diğer maddi bulgular birlikte değerlendirilmelidir. Aynı zararlı yazılımın veya aynı mixer hizmetinin kullanılması, tek başına belirli bir devleti ya da kişiyi kesin olarak göstermeye elverişli değildir.

9 Para hareketleri dondurma ve geri kazanım

9.1 İlk çıkış ile sonraki aklama aynı aşama değildir

İlk aşamada varlıklar borsayla ilişkilendirilen adreslerden saldırganla ilişkilendirilen adreslere gönderilir. İkinci aşamada varlıklar bölünebilir, başka varlıklarla takas edilebilir, farklı adresler veya köprüler üzerinden taşınabilir ya da borç verme protokollerinde teminat olarak kullanılabilir. Aynı varlığın farklı adresler arasında birden fazla kez hareket etmesi, her transferin yeniden ayrı zarar olarak toplanmasını gerektirmez.

TRM, Bitcoin ayağında 18.270 BTC'lik çıkışın ardından 1.000 ve 100 BTC gibi daha küçük çıktılara ayrılma gözlemlediğini bildirmektedir. Analizde kullanılan peel chain, tipik olarak bir UTXO işleminde tutarın bir bölümünün ayrılması ve kalan bölümün yeni bir adrese aktarılmasıyla yinelenebilen hareket zinciridir. Layering ise suç gelirinin izini karmaşıklaştırmaya yönelik daha geniş katmanlaştırma kavramıdır. Dağıtma veya smurfing belirli küçük işlemlere bölme yöntemlerini ifade edebilir; bu terimler her durumda eş anlamlı değildir. [5]

Yüklenen görseldeki “bir cüzdan, 10 cüzdan, her birinden 100 cüzdan” şeması, erişilen olay kaynaklarıyla kesin bir transfer sayısı olarak doğrulanamamıştır. On farklı ağda varlık çıkışı görülmesi de bütün fonların daha sonra on ağ arasında köprülenerek aktarıldığı anlamına gelmez. Öte yandan fonların bölünmesi iz sürmeyi güçleştirebilse de, izlemenin matematiksel veya adli bakımdan imkânsızlaştığını göstermez.

9.2 Dondurma iade ve zarar arasındaki fark

Binance yaklaşık 3 milyar dolarlık varlığın dondurulduğunu açıklamıştır. TRM'nin daha erken bir zaman kesiti için yayımladığı yaklaşık 2,7 milyar dolar sayısı ile Binance'in daha sonraki yaklaşık 3 milyar dolarlık açıklaması, farklı zaman ve kapsamlar nedeniyle birlikte değerlendirilmelidir. İki rakam toplanamaz. [2, 5]

Bir stablecoin sözleşmesindeki dondurma işlevi, ilgili tokenın belirli adresten aktarımını sınırlandırabilir; bir borsada hesaba bloke konulabilir veya ilgili ağın yönetişim yapısına bağlı başka tedbirler alınabilir. Fakat dondurma = zilyetliğin devri = mahkeme kararıyla müsadere = mağdura iade değildir. Her aşama farklı teknik ve hukuki koşullara tabidir.

BTC ve ETH gibi yerel varlıklar bakımından Tether veya Circle benzeri tek bir token ihraççısının sözleşme düzeyinde dondurma yetkisi bulunmaz. Bununla birlikte suç gelirinin merkezi bir borsaya veya kimliği belirlenmiş bir saklayıcıya ulaşması hâlinde hesap düzeyinde tedbir ve adli el koyma ihtimali ayrıca değerlendirilir. Bu nedenle “Bitcoin hiçbir koşulda dondurulamaz” ya da “tüm blokzincir transferleri aynı şekilde geri alınabilir” biçimindeki genellemeler hatalıdır.

9.3 DeFi ve piyasa aktörleri

TRM, bazı varlıkların piyasa yapıcılarla takas edildiğini ve stablecoin teminatı karşılığında bir borç verme protokolünden ETH temin edildiğini bildirmiştir. Böyle işlemler, dondurma öncesinde varlığın türünü veya üzerinde bulunduğu adresi değiştirerek müdahaleyi zorlaştırabilir. Bu veriden bütün piyasa yapıcıların suç ortağı olduğu, protokolün hacklendiği veya her karşı tarafın varlıkların kaynağını bildiği sonucu çıkmaz. [5]

10 Binance SAFU rezerv ve tazmin taahhüdü

Binance, olayın mali etkisini kullanıcılar yerine şirketin üstleneceğini; SAFU ve şirket kaynaklarını kullanacağını açıklamıştır. 30 Ekim güncellemesinde 6,34 milyar dolardan fazla kaynağın ayrıldığını, yaklaşık 5 milyar dolarlık ilgili varlıkla kaybın yaklaşık %80'inin karşılandığını belirtmiştir. 31 Ekim duyurusunda bu oranı yaklaşık %90 olarak güncellemiştir. Bunlar şirketin kendi beyanlarıdır ve kullanıcı başına tamamlanmış bir ödeme listesi değildir. [2, 3]

31 Ekim açıklamasında BTC, ETH, USDT, BNB, SOL, USDC, XRP, USD1, RLUSD ve ZEC için %100 karşılama beyan edilmiş; kalan yaklaşık %10'luk bölümde daha düşük likiditeli diğer varlıkların teminine çalışıldığı bildirilmiştir. Şirket, kaynaklar arasında kendi hazinesini ve vadeli işlem sigorta fonunun bir bölümünü saymış; SAFU'nun kısmen kullanılmasının izleyen 24 saat içinde beklendiğini belirtmiştir. Vadeli işlem sigorta fonu kullanımının kapsamı, kalan tampon ve aşırı piyasa koşullarındaki olası etkileri ayrıca izlenmelidir. [3]

SAFU bir mevduat sigortası değildir. Kapsamı, hukuki yapısı, güncel bakiyesi ve hangi zararları hangi şartlarla karşılayacağı ilgili açıklamalar ve uygulanabilir sözleşmelerle değerlendirilmelidir. Bir fonun varlığı, piyasa fiyatlarının düşmeyeceği veya bütün dolaylı zararların karşılanacağı anlamına gelmez. Ancak bu gözlemden somut bir kullanıcı zararının hangi tutarda doğduğu ya da tazmin edilmeyeceği de otomatik olarak çıkarılamaz.

11 Proof of Reserves neyi gösterir

Rezerv kanıtı veya Proof of Reserves, belirli bir tarih ve kapsam içinde açıklanan cüzdan bakiyeleri ile müşteri bakiyelerinin karşılaştırılmasına yönelik bir doğrulama yöntemidir. Merkle ağacı veya sıfır bilgi kanıtı, ilgili hesap bakiyesinin belirli bir veri kümesine dahil edilmesini ve yöntemin öngördüğü diğer matematiksel koşulları doğrulamaya yardımcı olabilir. Kullanıcının kendi kaydının ağaçta yer alması, tek başına tüm yükümlülüklerin eksiksiz raporlandığını veya adreslerdeki bütün varlıkların hukuken serbest ve rehin dışı olduğunu kanıtlamaz. [21, 22]

Binance, 31 Ekim 00.00 UTC itibarıyla yeni bir rezerv görüntüsü aldığını ve ilgili sayfayı güncellediğini açıklamıştır. Aynı duyuruda tam sıfır bilgi kanıtının hazırlanması için 3 Kasım 2026 hedefi verilmiştir. Dolayısıyla 31 Ekim tarihli görüntü ile daha sonra yayımlanacağı söylenen tam kanıt ayrı şeylerdir. [3]

Hukuken ve finansal olarak anlamlı bir değerlendirmede şu sorular sorulmalıdır: Görüntü hangi tüzel kişiyi, hangi müşteri hesaplarını ve hangi varlıkları kapsıyor? Borç, rehin, borç alınmış varlık ve ilişkili taraf işlemleri nasıl açıklanıyor? Adres kontrolü nasıl kanıtlanıyor? Yükümlülüklerin tamamı nasıl doğrulanıyor? Hesap bakiyesi bireysel olarak doğrulanabiliyor mu? İnceleme bağımsız denetçi tarafından hangi standart ve güvence düzeyiyle yapıldı? Bir anlık görüntü daha sonraki likiditeyi ve tüm bilanço risklerini kendi başına ortaya koyamaz. [21, 22]

12 Kullanıcılar ve piyasalar üzerindeki etkiler

12.1 Merkezi borsa kullanıcıları

Doğrudan kullanıcılar açısından risk; hesaplarında gösterilen varlık miktarının değişmesi, belirli çekimlerin geçici olarak yapılamaması, işlem emirlerinin yerine getirilememesi, fiyat oynaklığı veya sözleşmeye bağlı başka finansal sonuçlar şeklinde ortaya çıkabilir. Cüzdandan borsa düzeyinde yetkisiz çıkış yapılması, her kullanıcının bireysel hesabının hacklendiği veya kayıtlı bakiyesinin azaldığı anlamına gelmez.

Bir kullanıcının gerçek kaybı, saldırıdan önceki ve sonraki hesap dökümleri, bekleyen çekim talimatları, hesap içi kayıtlar, emir geçmişi, varlığın türü ve hizmet sözleşmesi birlikte incelenerek belirlenmelidir. Çekim yapılamaması da tek başına varlıkların kesin olarak kaybedildiğini göstermez; buna karşılık uzun süreli bir kesinti, somut koşullarda ayrıca incelenmesi gereken zararlara yol açabilir.

12.2 Binance TR kullanıcıları

Binance TR, kripto çekimlerinin geçici olarak durdurulduğunu; TL yatırma ve çekme, kripto yatırma ve alım satım dahil diğer belirttiği işlevlerin sürdüğünü duyurmuştur. Kullanıcılar yönünden sözleşmenin hangi tüzel kişiyle kurulduğu, varlıkların kim tarafından hangi modelle saklandığı ve ilgili işlem kayıtları önemlidir. Grup markasının ortak olması; global ve yerel şirketlerin bütün borçlarının, bütün saklama altyapılarının veya müşteri hesaplarının otomatik olarak özdeş olduğu anlamına gelmez. [4]

SPK'nın geçici faaliyet listesinde Binance Turkey Kripto Varlık Alım Satım Platformu AŞ yer almaktadır. SPK, aynı sayfada bu geçici listede bulunmanın tek başına mevzuat uyarınca yetkilendirildiği anlamına gelmediğini özellikle belirtmektedir. Bu nedenle şirketin güncel izin ve hizmet durumu ayrıca ve doğru liste üzerinden kontrol edilmelidir. [15]

12.3 Fiyatlar ve likidite

Reuters'in olay sonrası piyasa haberine göre Bitcoin 77.646 dolar düzeyine kadar gerilemiş; aynı haberde ETH için 2.238,76 dolar ve BNB için yaklaşık 694 dolar seviyelerinden söz edilmiştir. Bunlar ilgili haberin zamanına özgü gözlemlerdir, güncel fiyat veya kalıcı seviye olarak kullanılmamalıdır. Saldırı haberi ile fiyat hareketleri arasında zaman bakımından ilişki bulunması, düşüşün tamamının yalnızca bu olaydan kaynaklandığını matematiksel olarak ispatlamaz. [10]

Özellikle volatilite arttığında alış-satış farkı açılabilir, emir defteri derinliği azalabilir, piyasa emirleri beklenenden farklı fiyattan gerçekleşebilir ve vadeli işlemlerde teminat seviyesi bozulabilir. Kullanıcı çekim yapamıyorsa pozisyonunu başka platformda dengeleme imkânı da daralabilir. Kaldıraçlı kullanıcılar yönünden likidasyon ve otomatik pozisyon azaltımı riskleri ürün koşullarıyla birlikte ayrıca değerlendirilmelidir.

12.4 Diğer borsalar ve finansal kuruluşlar

Piyasa yapıcılar, stablecoin ihraççıları, saklama hizmeti veren kurumlar ve saldırganla ilişkili adreslerden varlık kabul etmiş olabilecek platformlar, karşı taraf ve uyum riski yaşayabilir. Bununla birlikte bir adrese dolaylı temas tespit edilmesi, fonun mutlaka suç geliri olduğunu veya hesabın sahibinin suç işlediğini göstermeyebilir. İşlemin miktarı, yönü, kaç aracı kullanıldığı ve kaynak verisinin güvenilirliği değerlendirilmelidir.

Bankaların tamamının veya geleneksel finans altyapısının %70'inin bu saldırı nedeniyle tehlikede olduğu iddiası sunulan materyallerde kaynaklandırılmamıştır. Binance olayından hareketle böyle bir oran veya bankacılık sisteminin çökeceği sonucu çıkarılamaz.

13 Türkiye bakımından hukuki değerlendirme

13.1 Öncelikle uygulanacak ilişkinin tespiti

Türkiye'deki bir müşteri açısından hukuki analiz; hesabın hangi tüzel kişi nezdinde açıldığı, sözleşmenin tarafları, işlemin ve saklamanın kim tarafından gerçekleştirildiği, uygulanacak hukuk, hizmetin niteliği ve somut zararın ne olduğunun tespitiyle başlar. Bir kullanıcının global platformda, yerel platformda veya her ikisinde hesabı bulunabilir. Bu farklı ilişkiler tek bir sözleşme gibi ele alınmamalıdır.

6362 sayılı Sermaye Piyasası Kanunu'nda 7518 sayılı Kanun ile kripto varlık hizmet sağlayıcılarına ilişkin düzenlemeler getirilmiştir. SPK, 13 Mart 2025'te III-35/B.1 ve III-35/B.2 sayılı iki temel tebliği yayımladığını; bunların kuruluş, faaliyet, iç kontrol, bilgi sistemleri, saklama, transfer ve sermaye yeterliliği gibi başlıkları düzenlediğini açıklamıştır. Somut uyuşmazlıkta tebliğlerin ve ilgili kararların olay tarihindeki güncel metni ve geçiş hükümleri kontrol edilmelidir. [13, 14]

13.2 Siber saldırı kaynaklı varlık kaybı

6362 sayılı Kanun'un 99/A maddesinin dördüncü fıkrası, hizmet sağlayıcıların bilişim sistemlerinin işletilmesi, siber saldırı, bilgi güvenliği ihlali veya personel davranışlarından kaynaklanan kripto varlık kayıpları bakımından 6098 sayılı Türk Borçlar Kanunu'nun 71. maddesi kapsamında sorumluluk düzeni öngörür. Kayıp hizmet sağlayıcıdan tazmin edilemez veya edilemeyeceği açıkça belli olursa, mensupların kusurlarına ve somut şartlara göre, kendilerine yüklenebilen ölçüde kişisel sorumluluğu da gündeme gelebilir. Hükmün olaya uygulanabilmesi için ilgili tüzel kişi, uygulanabilir hukuk ve kayıp ile olay arasındaki bağ ayrıca incelenmelidir. [14]

Aynı fıkra, hizmet sağlayıcının kusuru bulunmaksızın yaşanan hizmet kesintisi nedeniyle belirli süre emir iletilememesi veya işlem ve transfer yapılamaması gibi durumlarda ortaya çıkan zararların bu özel fıkra kapsamında değerlendirilmeyeceğini belirtir. Bu istisna her kesintide sağlayıcının otomatik olarak sorumsuz olduğu, başka hiçbir hukuki talebin ileri sürülemeyeceği veya her fiyat düşüşünün otomatik olarak tazmin edileceği anlamına gelmez. Kusur, sözleşme, uygun illiyet bağı, zararın ispatı ve diğer ilgili hükümler somut dosyada ayrıca değerlendirilir. [14]

13.3 Varlığın değeri ile varlığın miktarı

Kullanıcının hesabındaki 1 BTC miktarının eksilmesiyle, 1 BTC miktarı aynı kalmasına rağmen piyasa değerinin düşmesi farklı zarar senaryolarıdır. Birinci durumda varlık miktarındaki eksilme ve bunun nedeni; ikinci durumda ise fiyat hareketi, ifa edilemeyen emir, hizmet kusuru ve zararın nasıl hesaplanacağı incelenir. Örneğin çekim gecikmesinde zararın hesabı için, ilgili ağın açık olduğu zaman, kullanıcının geçerli çekim talimatı, işlemin normal koşullarda tamamlanma süresi ve makul alternatifler gibi unsurlar önem taşıyabilir. Fiyat düşüşünün varlığı tek başına sağlayıcının sorumluluğunu ispatlamaz.

13.4 Kişisel veriler

Sıcak cüzdanlardan yetkisiz transfer yapılması, kullanıcıların kimlik belgeleri veya kişisel verilerinin de sızdırıldığını tek başına göstermez. Ayrı bir kişisel veri ihlali tespit edilirse, ilgili veri sorumlusunun niteliği ve olayın kapsamı çerçevesinde 6698 sayılı Kanun ve KVKK kararları değerlendirilir. KVKK'nın 2019/10 sayılı kararına ilişkin açıklamasında, belirli nitelikteki ihlallerin öğrenilmesinden itibaren en geç 72 saat içinde Kurula bildirilmesi ve ilgili kişilerin uygun biçimde bilgilendirilmesi düzeni açıklanmaktadır. Somut olayda kişisel veri ihlali bulunduğu veya her global şirket için aynı yükümlülüğün otomatik doğduğu varsayılmamalıdır. [16]

14 Dijital delil ve uzman incelemesi

Bir ceza soruşturması, hukuk uyuşmazlığı veya uzman mütalaasında inceleme aşağıdaki veri kümelerini birlikte ele almalıdır. İnceleme yetkisi bulunmayan kişilerden gizli anahtar, kurtarma ifadesi veya gizli kullanıcı kimlik bilgileri istenmemeli; delil temini yetkili makam ve uygun hukuki süreç üzerinden yürütülmelidir.

1. Zincir üstü kayıtlar: Ağ, blok numarası ve blok hash'i, işlem hash'i, işlem sırası, olay günlükleri, iç çağrı izleri, token transferleri, sözleşme bytecode'u, yetkilendirme listesi, nonce ve zaman bilgisi. İşlem hash'i ile cüzdan adresi karıştırılmamalıdır.

2. İmza ve anahtar kayıtları: İmzalama talebini oluşturan servis, talep içeriği, politika motoru kararı, bağımsız onaylar, HSM veya MPC denetim kayıtları, işlem kimliği ve zaman damgası. İmza talebi ile anahtarın dışarı sızması birbirinden ayrılmalıdır.

3. Kurumsal erişim kayıtları: Kimlik sağlayıcı, ayrıcalıklı erişim, VPN, uç nokta algılama, servis hesabı, konteyner ve orkestrasyon kayıtları, CI/CD değişiklikleri, bulut erişim ve güvenlik olayları.

4. Uç nokta delilleri: Yetkili süreç çerçevesinde uçucu bellek ve disk imajı, dosya ve süreç zaman çizelgesi, tarayıcı ve oturum verileri, sistem günlüğü, şüpheli dosyalar, komut geçmişi ve ağ bağlantıları.

5. Müşteri kayıtları: Hesap açılış ve sözleşme belgeleri, olay öncesi ve sonrası hesap özeti, varlık türü ve miktarı, bekleyen çekimler, emirler, destek başvuruları ve yanıtlara ilişkin tarihli kayıtlar.

6. Üçüncü taraf kayıtları: Token ihraççısı dondurma kayıtları, borsa ve saklayıcı cevabı, mümkünse zincir üstü adres sahipliği ve KYC verileri, adli yardımlaşma yanıtları ve ilgili tedbir kararları.

Delillerin temin tarihi, kaynağı, imaj alma yöntemi, kullanılan araç ve sürüm, hesaplanan SHA-256 gibi bütünlük değerleri ve her teslim alan kişi belgelenmelidir. Zincir üstü verilerde de kullanılan düğüm veya servis sağlayıcı, blok yüksekliği, ağ adı ve olası zincir yeniden düzenlemeleri kayda geçirilmelidir. İlgili çalışma kayıtlarının ve menşe bilgisinin korunması, NIST olay müdahalesi rehberindeki yaklaşım ile uyumludur. [18]

Açık blokzincir verisi ile borsanın kapalı iç kayıtları birlikte değerlendirilmeden, bir toplu cüzdandan çıkan belirli tokenların hangi bireysel müşteriye ait olduğunu kesin biçimde söylemek çoğu durumda mümkün değildir. Aynı şekilde bir adresin analiz şirketi tarafından belirli bir borsaya veya faile etiketlenmesi, etiketin dayandığı yöntem incelenmeden tartışmasız maddi gerçek kabul edilmemelidir.

Örnek zincir üstü inceleme bağlantıları

Blockaid'in yayımladığı teknik rapor, Binance 14 adresi, saldırganla ilişkilendirdiği sözleşme ve yetkilendirme işlemlerine bağlantı vermektedir. Bunlar araştırma ve doğrulama amaçlıdır; bu adreslere varlık gönderilmemelidir. İnceleme sırasında kullanılan blok gezgini sayfaları bu rapor hazırlanırken otomatik erişim engeli verdiğinden, ilgili işlem ayrıntıları doğrudan bağımsız olarak yeniden doğrulanamamış; bilgiler Blockaid'in yayımladığı analiz üzerinden aktarılmıştır. [6]

Binance 14 adresi: 0x28C6c06298d514Db089934071355E5743bf21d60

Blockaid tarafından operatör olarak etiketlenen adres: 0x7C8601d4645b93cea45F71e118A729332e6B5CA0

Blockaid tarafından sözleşme olarak gösterilen adres: 0x63e842B054Bd624a465454D533C33F573e9c6fAe

Yetkilendirme işlem hash'i: 0xad99264d5532ae0dd04b2004eebda05f25657e70dacb764f7ac8d4ccd051298b

İlk büyük süpürme işlem hash'i: 0x53bd38b816c23e74134786c29a8c18d792777998a3b9326047b583100e88e2f3

Adres veya işlem hash'inin tam karakter dizisi doğrulanmalı; kısa önek ve son ek benzerliğiyle kimlik eşleştirmesi yapılmamalıdır. Blockaid'in dinamik takip sayfası yalnızca yayımladığı kapsamı gösterir; sayfada eşleşme bulunmaması kesin olarak risk bulunmadığını kanıtlamaz. [7]

15 Saldırı sonrasında bireysel korunma

15.1 Hesabı ve iletişim kanalını güvenceye alın

Platforma reklam bağlantısı veya gelen mesaj üzerinden değil, kullanıcının daha önce doğruladığı uygulama ya da adres üzerinden girilmelidir. Olay sonrasında “varlığınızı kurtaracağız”, “rezervinizi doğrulayın”, “cüzdanınızı eşitleyin” veya “hesabınız kapatılacak” temalı dolandırıcılık mesajları gönderilebilir. Hiçbir meşru destek süreci kurtarma kelimelerinin, özel anahtarın veya tek kullanımlık doğrulama kodunun üçüncü kişiye verilmesini gerektirmez.

Borsada destekleniyorsa FIDO2/WebAuthn güvenlik anahtarı veya uygun geçiş anahtarı kullanılması, kimlik avına karşı güçlü bir seçenektir. TOTP uygulaması çoğu durumda SMS'e göre SIM değiştirme riskini azaltabilir; ancak sahte siteye manuel girilen TOTP kodu gerçek zamanlı oltalamayla ele geçirilebilir. Push bildirimleri de yanlış onay ve bildirim yorgunluğu riski taşır. Bu nedenle “Authenticator kullanmak her türlü

oltalamayı önler” denilemez. [17]

E-posta hesabı ayrı ve benzersiz parolayla korunmalı; borsa hesabında tanınmayan cihaz ve oturumlar kapatılmalı; API anahtarları, para çekme izinleri ve beyaz liste ayarları gözden geçirilmelidir. Kullanılmayan API anahtarları iptal edilmeli; gereken anahtarlarda para çekme yetkisi kapatılmalı ve mümkünse IP kısıtlaması uygulanmalıdır. Yeni çekim adresi eklenmesi, parola değişimi ve büyük işlemler için bildirimler açılmalıdır.

15.2 Soğuk cüzdan ve kişisel saklama

Kişisel saklama, borsanın saklama ve hizmet kesintisi risklerine maruziyeti azaltabilir; fakat kurtarma kelimelerinin kaybı, sahte donanım, yanlış ağ seçimi, zararlı işlem imzası, cihaz tedarik zinciri, fiziksel zorlama ve miras planlaması gibi yeni riskler doğurur. “Soğuk cüzdan mutlak güvenlik sağlar” ifadesi isabetli değildir.

Donanım cüzdanı doğrudan güvenilir satıcıdan edinilmeli; kurtarma ifadesi cihazın güvenilir kurulum akışında çevrim dışı oluşturulmalı ve fotoğraf, e-posta veya buluta yüklenmemelidir. Kullanıcıya basılı halde verilmiş bir kurtarma ifadesi kullanılmamalıdır. Alıcı adresi ve seçilen ağ cihaz ekranında ayrıca doğrulanmalı; önce küçük bir test transferi yapılmalı, ağ ücretleri ve borsanın desteklediği ağlar kontrol edilmelidir. Cihazın internete bağlı bilgisayarla kullanılması tek başına cihazın tüm anahtarlarının otomatik biçimde çevrim içi olduğu anlamına gelmez; buna karşılık kullanıcı kötü niyetli bir yetkilendirmeyi onaylarsa donanım cüzdanı da zararlı işlemi engelleyemeyebilir.

Varlıkların tamamını tek bir borsada veya tek bir kişisel cüzdanda tutmak yoğunlaşma riski yaratabilir. Makul dağılım, kişinin teknik yetkinliğine, güvenli yedekleme kapasitesine, işlem ihtiyacına ve risk toleransına bağlıdır. Olayı gerekçe göstererek otomatik biçimde altın, gümüş veya herhangi bir ürüne geçilmesi gerektiği sonucu çıkarılamaz.

15.3 Kullanıcı zararını belgeleme

Hesap bakiyesi ve işlem geçmişi, desteklenen resmi dışa aktarma seçeneğiyle tarihli olarak alınmalı; çekim talebi veya hata ekranları mümkünse işlem kimliği ve zaman bilgisiyle birlikte saklanmalıdır. Belge üzerinde sonradan düzenleme yapılacaksa orijinal örnek korunmalı, gerekirse hash değeri hesaplanmalıdır. Destek başvurusu ve alınan yanıtlar tek bir dosyada tutulmalı; kişisel veriler paylaşılırken gereksiz kimlik ve hesap bilgilerinin açığa çıkması önlenmelidir.

16 Kurumsal güvenlik ve olay müdahalesi

16.1 İlk 24 saat için öncelikler

Yetkisiz işlem şüphesinde riskli çekim yolları ve etkilenen yetkilendirmeler kontrollü biçimde durdurulmalı; cüzdanın kod ve yetki durumu, müşteri fonları ve yüksek riskli servisler ayrıştırılmalıdır. Eş zamanlı olarak uçucu delillerin kaybı dikkate alınarak olay müdahale ekibi tarafından bellek, günlük ve yapılandırma kayıtları korunmalıdır. Sistemi hemen kapatmanın bazı aktif saldırıları durdurabilmesi yanında uçucu delilleri silebileceği de hesaba katılmalıdır; karar olayın özelliğine göre verilir. [18]

Adres, token ve ağ bazında dondurma veya hesap tedbirleri için ilgili ihraççılar, hizmet sağlayıcıları ve yetkili makamlarla koordinasyon kurulmalı; her dondurmanın zamanı, kapsamı ve hukuki dayanağı kaydedilmelidir. Müşteri iletişiminde “tespit edildi”, “donduruldu”, “geri kazanıldı”, “yerine konuldu” ve “kullanıcıya ödendi” ayrı kategoriler halinde açıklanmalıdır.

16.2 İmzalama mimarisi

İmzalama servisi ile işlem talebi oluşturan servis ayrı güven sınırlarında çalıştırılmalı; kritik hedefler için bağımsız politika motorları ve insan onayları kullanılmalıdır. Tek bir cihaz, kimlik veya servis hesabının birden fazla zincirde sınırsız çekim yetkisine ulaşması engellenmeye çalışılmalıdır. MPC veya çoklu imza kullanılması tek başına yeterli değildir; aynı saldırganın bütün imza katılımcılarını, onay akışını veya politika motorunu etkileyip etkilemediği önemlidir.

Ağ ve varlık bazında işlem ve zaman penceresi limitleri; ilk kez görülen hedeflere gecikme; acil durdurma; sıcak cüzdan bakiyesi üst sınırı; yüksek tutarlı işlemlerde bağımsız doğrulama; EIP-7702 ve benzeri delegasyonların varsayılan olarak reddi; imza öncesi işlem simülasyonu ve cüzdan kod değişikliği uyarıları birlikte ele alınmalıdır. Güvenliğin maliyeti ile gerçek zamanlı hizmet sunumu arasında tercih yapılırken bu kontrollerin atlatılabileceği acil durum kanalları da test edilmelidir.

16.3 Kimlik uç nokta ve sıfır güven

Ayrıcalıklı personele phishing dirençli kimlik doğrulama, sadece ihtiyaç duyulan süre ve kapsamda yetki, ayrı yönetici cihazları, güçlü oturum yönetimi ve kritik onaylarda görev ayrılığı uygulanmalıdır. Servis kimlikleri ve kısa süreli erişim belirteçleri düzenli envanterlenmeli; bulut ve konteyner izinleri daraltılmalı; imaj bütünlüğü ve yazılım tedarik zinciri doğrulanmalıdır. Sıfır güven, tek bir ürün veya “giriş yapan herkesi sürekli yeniden doğrulama” sloganı değil; kimlik, cihaz, kaynak ve bağlam üzerinden erişim kararlarının tasarlandığı mimari bir yaklaşımdır. [19]

EDR, SIEM ve olay yönetimi sistemleri faydalıdır; ancak kurulu olmaları tek başına erken tespit veya otomatik müdahale garantisi vermez. Operasyon ekibinin on-chain değişiklikleri hangi eşiklerde nasıl karşılayacağı, 7/24 alarm sorumluluğu, tatbikatlar ve bağımsız test sonuçları önem taşır.

17 Geleceğe ilişkin olası senaryolar

Olumlu senaryo: Binance kalan varlıkları yerine koyar, ilgili kanıtları ve bağımsız inceleme kapsamını açıklar, çekimler güvenli biçimde kademeli olarak açılır ve dondurulan varlıkların bir kısmı hukuki süreçlerle geri kazanılır. Bu, kullanıcılara yönelik doğrudan kayıpların sınırlanmasına yardımcı olabilir; piyasa fiyatlarının belirli bir yöne gideceğini garanti etmez.

Ara senaryo: Çekimler ağlara ve varlıklara göre farklı hızlarda açılır; düşük likiditeli varlıkların yerine konulması uzar; dondurulmuş varlıkların iadesi farklı yargı bölgelerindeki işlemler nedeniyle aylar veya daha uzun sürebilir. Rezerv kanıtı yayımlansa da tam bilanço ve olayın kök nedeni yönünden yeni sorular devam edebilir.

Olumsuz senaryo: Yeni ihlal göstergeleri veya hizmet kesintileri ortaya çıkabilir; çalınan varlıkların bir bölümü başka varlıklara çevrilerek aklanabilir; operasyonel maliyetler, müşteri güveni ve piyasa likiditesi üzerinde ek baskı oluşabilir. Bunlar öngörü senaryolarıdır; somut olayda gerçekleşecekleri söylenemez.

Yakın dönemde dört unsur düzenli izlenmelidir: Binance ve Binance TR'nin çekim duyuruları; rezerv kanıtının kapsamı ve bağımsız doğrulaması; dondurulan varlıkların ne kadarının fiilen geri alındığı; şirketin söz verdiği teknik kök neden ve iyileştirme raporu. Ayrıca olası düzenleyici açıklamalar ve kullanıcı bazlı hizmet şikâyetleri takip edilmelidir.

18 Yüklenen materyallerde düzeltilmesi gereken hususlar

19 Sonuç ve takip planı

Binance saldırısı, kamuya açıklanan verilere göre çok büyük tutarlı bir sıcak cüzdan ve işlem yetkilendirme ihlalidir. Ethereum ayağında EIP-7702 delegasyonu, diğer çeşitli ağlarda geçerli imzalı transferler ve bazı varlıkların sonradan dondurulması teknik incelemenin merkezindedir. Bununla birlikte olayın başlangıç vektörü, erişilen tüm sistemler, imza üretiminin tam koşulları ve hukuki fail atfı bakımından nihai değerlendirme henüz tamamlanmamıştır.

Bireysel kullanıcılar açısından ilk adım, resmi kanallardaki hizmet durumunu kontrol etmek, hesap ve e-posta güvenliğini güçlendirmek, işlem ve bakiye kayıtlarını korumak, herhangi bir çekim veya saklama kararını kendi koşullarını değerlendirerek vermektir. Hukuki uyuşmazlık ihtimalinde ise ilgili tüzel kişi, sözleşme, varlık miktarındaki gerçek eksilme, hizmet kesintisinin nedeni ve ileri sürülen zararın ispatı ayrı ayrı belirlenmelidir.

Ek kaynaklar ve Binance'in sonradan yayımlayacağı teknik rapor temin edildiğinde; ilk erişim, etkilenen anahtar ve onay mimarisi, varlık iadesi ve Türkiye'deki kullanıcıların durumu bakımından bu rapor güncellenmelidir.

20 Kaynakça

[1] Binance, Security Incident Update, 30 Ekim 2026. İlk olay açıklaması ve DevOps bilgisayarı ihtimali. Kaynağı aç

[2] Binance, Security Incident Update 2, 30 Ekim 2026. Kayıp, dondurma, ilk karşılama ve iyileştirme açıklaması. Kaynağı aç

[3] Binance, Recovery Update 3, 31 Ekim 2026. Yaklaşık yüzde 90 yerine koyma, fon kaynakları ve rezerv görüntüsü. Kaynağı aç

[4] Binance TR, Kripto Varlık Çekimleri Hakkında Bilgilendirme, 30 Ekim 2026. Kaynağı aç

[5] TRM Labs, North Korea Steals USD 6.36 Billion From Binance in the Largest Hack in History, olayın teknik akışı, varlık dağılımı ve atıf değerlendirmesi. Kaynağı aç

[6] Blockaid, Binance Hack teknik incelemesi, EIP-7702, nonce ve işlem bağlantıları. Şirket kendi güvenlik hizmetlerini de tanıtmaktadır. Kaynağı aç

[7] Blockaid, Binance Hack Risk Exposure, dinamik adres ve varlık akışı görünümü. Kapsam ve zaman etiketi sayfadan kontrol edilmelidir. Kaynağı aç

[8] Ethereum Improvement Proposals, EIP-7702 Set Code for EOAs, teknik standart metni. Kaynağı aç

[9] Binance News, Richard Teng açıklaması, imzalama kontrolleri ve olay sonrası değerlendirme. Kaynağı aç

[10] Reuters, Bitcoin ve diğer kripto varlık fiyatlarında olay sonrası düşüş, 30 Ekim 2026; StreetInsider yeniden yayımı. Kaynağı aç

[11] Reuters, Binance saldırısına sektörün güvenlik tepkisi, 31 Ekim 2026. Kaynağı aç

[12] Associated Press, Binance saldırısına ilişkin genel olay özeti, 30 Ekim 2026. Kaynağı aç

[13] Sermaye Piyasası Kurulu, Kripto Varlık Hizmet Sağlayıcılarına İlişkin İki Tebliğ Yayımlandı, 13 Mart 2025; tebliğ metinlerine bağlantılar içerir. Kaynağı aç

[14] Resmî Gazete, 7518 sayılı Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun, 2 Temmuz 2024. Olay tarihindeki güncel konsolide metin ayrıca kontrol edilmelidir. Kaynağı aç

[15] Sermaye Piyasası Kurulu, Kripto Varlık Hizmet Sağlayıcılar Faaliyette Bulunanlar Geçici Listesi. Listede yer almak yetkilendirme anlamına gelmez. Kaynağı aç

[16] Kişisel Verileri Koruma Kurumu, kişisel veri ihlal bildirimi ve 2019/10 sayılı karar hakkında kamuoyu duyurusu. Kaynağı aç

[17] NIST, SP 800-63B-4 Digital Identity Guidelines Authentication and Authenticator Management, Temmuz 2025. Kaynağı aç

[18] NIST, SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management, Nisan 2025. Kaynağı aç

[19] NIST, SP 800-207 Zero Trust Architecture. Kaynağı aç

[20] FBI, North Korea Responsible for 1.5 Billion Dollar Bybit Hack, 26 Şubat 2025. Önceki olay bağlamındadır; Binance olayına dair kesin yargı kararı değildir. Kaynağı aç

[21] Binance Academy, What Is Proof of Reserves and How It Works, yöntemin açıklaması ve sınırları. Kaynağı aç

[22] U.S. Securities and Exchange Commission, The Potential Pitfalls of Purported Crypto Assurance Work, 27 Temmuz 2023. Kaynağı aç

[23] Binance Proof of Reserves resmî sayfası. Anlık görüntünün tarihi, dahil edilen varlıklar ve yöntemi ayrıca kontrol edilmelidir. Kaynağı aç

[24] CISA, FBI ve ABD Hazine Bakanlığı, TraderTraitor Kuzey Kore bağlantılı APT tehdidine ilişkin ortak uyarı. Genel tehdit arka planı olup bu olaya ilişkin kesin fail kanıtı değildir. Kaynağı aç

[25] Ethereum blok gezgini, Blockaid'in tanımladığı yetkilendirme işlemi. Otomatik erişimde 403 hatası alındığından bağımsız doğrulama gereklidir. Kaynağı aç

[26] Ethereum blok gezgini, Blockaid'in tanımladığı ilk büyük transfer. Otomatik erişimde 403 hatası alındığından bağımsız doğrulama gereklidir. Kaynağı aç

[27] U.S. Securities and Exchange Commission, rezerv kanıtı ile finansal tablo denetimi arasındaki sınırlara değinen dava belgesi. Kaynağı aç

[28] Sermaye Piyasası Kurulu, güncel mevzuat sistemi; III-35/B.1 ve III-35/B.2 tebliğlerinin güncel metinleri ve ilgili kararlar. Kaynağı aç

Olay kronolojisi — kaynak rapordaki tablo

Tarih ve saat | Gelişme

28 Ekim 2026 ve öncesi | TRM'ye göre saldırganla ilişkilendirilen operatör adresine küçük tutarlı aktarımlar yapıldı; zincir üstü hazırlık en az 36 saat öncesine uzanıyordu.

29 Ekim 23.05 | XRP Ledger üzerindeki Binance cüzdanlarından yetkisiz çıkışların başladığı bildirildi; şirket de saldırının başlangıcını yaklaşık 20.05 UTC olarak verdi.

29 Ekim 23.20.59 | Blockaid'e göre Ethereum'da 50 EIP-7702 yetkilendirmesi içeren işlem yayımlandı.

29 Ekim 23.24.23 | Aynı kaynağa göre Binance 14 adresi üzerinden büyük tutarlı ilk Ethereum boşaltması gerçekleşti.

29 Ekim 23.41 civarı | Devredilmiş yetkilerin ilişkili akıllı hesap üzerinden USDC aktarımında da kullanıldığı belirtildi.

30 Ekim 00.44 civarı | Daha sonra cüzdana gelen varlıkların yeniden çekildiği Blockaid tarafından raporlandı.

30 Ekim 02.05 civarı | TRM'ye göre Avalanche ve Polygon üzerinde daha sonraki bir transfer dalgası izlendi. Bu nedenle tüm tutarın yalnızca 20 dakikada çıktığı söylenemez.

30 Ekim | Binance yaklaşık 6,3 milyar dolar etki ve 3 milyar dolar dondurma açıkladı; Binance TR kripto çekimlerine ilişkin geçici tedbiri duyurdu.

31 Ekim | Binance, etkilenen tutarın yaklaşık %90'ının ilgili varlıklarla yerine konulduğunu, rezerv görüntüsünün alındığını ve çekimlerin 1 Kasım'da yeniden açılmasının hedeflendiğini bildirdi.

Varlıkların ağlara göre dağılımı — kaynak rapordaki tablo

Ağ veya ağ grubu | Yaklaşık çıkış | Açıklama

Ethereum | 3,79 milyar dolar | ETH ve USDT, USDC, RLUSD dahil çok sayıda token.

Bitcoin | 1,47 milyar dolar | Yaklaşık 18.270 BTC.

Tron | 628 milyon dolar | Yaklaşık 612,7 milyon USDT ve 46,4 milyon TRX.

XRP Ledger | 296 milyon dolar | Yaklaşık 233,46 milyon XRP.

Solana | 96 milyon dolar | Yaklaşık 970.500 SOL.

Arbitrum, Optimism ve Base | Toplam 39 milyon dolar | TRM'nin ilgili ağ grubu için yaklaşık hesaplaması.

Avalanche | 28 milyon dolar | Yaklaşık değer.

Polygon | 10 milyon dolar | Yaklaşık değer.

Kaynak materyalde düzeltilmesi gereken iddialar

Yüklenen materyaldeki ifade | Bilimsel ve hukuki değerlendirme

63,3 milyar dolar çalındı veya risk oluştu | Binance'in tahmini yaklaşık 6,3 milyar dolar; TRM'nin işlem anı hesaplaması yaklaşık 6,36 milyar dolardır.

Saldırı tamamen tek mühendisin bilgisayarından başladı | İlk bulguda dizüstü bilgisayar ihtimali belirtilmiş, daha sonra ek ihlal noktaları açıklandığı bildirilmiştir; tam kök neden yayımlanmamıştır.

Özel anahtar sızmadı, dolayısıyla imza sistemi güvenlidir | Anahtarın dışarı sızmaması ile yetkisiz imza ürettirilmesi farklı sorulardır; ikincisi teknik olarak mümkündür.

Tüm fonlar 20 dakikada boşaltıldı | TRM, büyük bölümün yaklaşık 20 dakikada aktarıldığını; daha sonraki ağ hareketlerini de bildirmektedir.

Bir cüzdandan 10, her birinden 100 cüzdana dağıtıldı | Erişilen birincil olay raporlarında bu kesin sayı düzeni doğrulanmamıştır.

Çirkinleme, çirinleme ve smurfing aynı yöntemdir | Kaynaklarda Bitcoin ayağı için peel chain, daha geniş bağlamda layering gibi farklı teknikler yer almaktadır.

Blokzincirde dondurma veya geri kazanım mümkün değildir | İhraççı kontrollü tokenlarda dondurma ve bazı ağ veya platformlarda tedbir mümkündür; geri kazanım ayrıca süreç gerektirir.

SAFU tüm anaparayı mutlaka karşılar | Binance'in kayıpları karşılama taahhüdü vardır; kapsam, hukuki kaynak ve fiilî yerine getirme ayrıca değerlendirilmelidir.

Yapay zekâ Binance saldırısını gerçekleştirdi | Erişilen bulgular bu olayın saldırganlarca yapay zekâ kullanılarak yapıldığını doğrulamamaktadır; Blockaid'in kendi tespit araçlarında yapay zekâdan yararlanması ayrı bir konudur.

Küresel bankacılık altyapısının %70'i PHP nedeniyle risk altında | Kaynak gösterilmemiştir ve olayla nedensel bağlantısı doğrulanmamıştır.