Sayı 23
04.08.2026

BÜYÜK ÖLÇEKLİ BİR KRİPTO VARLIK AKLAMA AĞININ ÇÖKERTİLMESİ: AUDIA6 OPERASYONUNDAN TEMEL ÇIKARIMLAR

Suçtan kaynaklanan 336 milyon avronun üzerindeki kripto varlığın aklanmasında kullanıldığı değerlendirilen AudiA6, koordineli bir uluslararası soruşturma sonucunda çökertilmiştir. AudiA6'nın, fidye yazılımı grupları ve diğer siber suç ağları tarafından suçtan elde edilen kripto varlıkların kaynağını, mülkiyetini ve hareketlerini gizlemek amacıyla kullanıldığı ileri sürülmektedir.

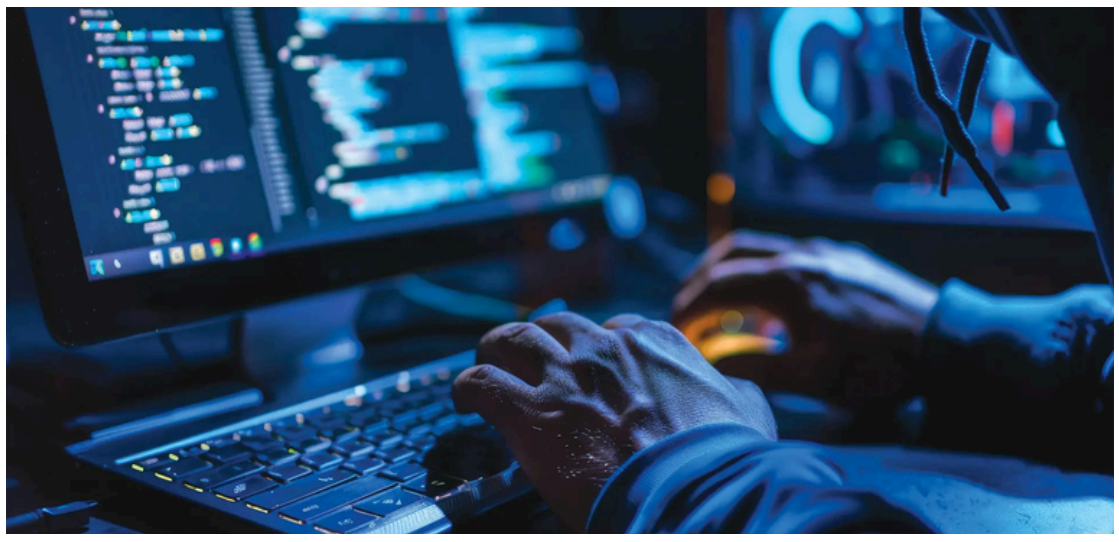
AudiA6'nın çökertilmesi, yalnızca belirli bir aklama servisinin faaliyetlerinin sona erdirilmesiyle sınırlı kalmamıştır. Operasyonla aynı zamanda yüz milyonlarca avro tutarındaki suç gelirinin aktarılması, gizlenmesi ve yeniden finansal sisteme dâhil edilmesinde kullanıldığı değerlendirilen daha geniş bir dijital ve finansal altyapı hedef alınmıştır. Bu yönüyle AudiA6 vakası; finansal soruşturmaların, siber suçlarla mücadele yöntemlerinin, dijital delil incelemelerinin, sınır ötesi adli iş birliğinin ve malvarlığının güvence altına alınmasına yönelik tedbirlerin karmaşık kripto varlık soruşturmalarında nasıl birlikte işletilebileceğini gösteren önemli bir örnek oluşturmaktadır.

I. AudiA6'nın Aklama Modeline İlişkin İddialar

AudiA6'nın, suçtan kaynaklanan kripto varlıkların kaynağını gizlemek isteyen kişiler ile yasal kripto varlık ekosistemi içerisinde açılmış hesaplar arasında aracı olarak faaliyet gösterdiği ileri sürülmektedir. Kullanıcıların, aynı organizasyon tarafından işletildiği değerlendirilen Dark2Web adlı siber suç forumu ile özel mesajlaşma platformları üzerinden AudiA6'ya yönlendirildiği belirtilmektedir.

Hizmetten yararlanmak isteyen kullanıcılar, kripto varlıklarını kendi özel cüzdanlarından AudiA6'nın kontrolündeki cüzdanlara aktarmıştır. Fonlar daha sonra çok sayıda küçük işleme bölünmüş ve çalınmış veya ticari yollarla edinilmiş kimlikler kullanılarak açılan çeşitli aracı hesaplar üzerinden transfer edilmiştir. Bu katmanlandırma işlemlerinin ardından fonlar yeniden bir araya getirilerek sözde "temizlenmiş" kripto varlıklar şeklinde kullanıcının cüzdanına iade edilmiştir.

AudiA6'nın söz konusu hizmet karşılığında %3 ila %10 arasında komisyon aldığı ileri sürülmektedir. Bu işlem yapısının; fon hareketlerini karmaşıklaştırmayı, suç geliri ile kaynağı arasındaki bağlantıyı zayıflatmayı ve fonların nihai kullanıcısının tespitini güçleştirmeyi amaçladığı değerlendirilmektedir. Vaka, kripto varlık aklama servislerinin blokzincir üzerindeki transferleri, kimliklerin kötüye kullanımını, aracı hesapları ve yasal kripto varlık platformlarını birlikte kullanarak gerçek faydalanıcının ve fonların kaynağının gizlenmesini sağlayabildiğini göstermektedir.



II. Soruşturmanın Genişletilmesi

Amerika Birleşik Devletleri Gizli Servisi ile Amerikan Gelir İdaresi Ceza Soruşturmaları Birimi'nin AudiA6'yı 2022 yılından itibaren soruşturduğu belirtilmektedir. 2022–2026 yılları arasında gerçekleştirilen gizli soruşturma işlemlerinde AudiA6'nın; fidye yazılımı faaliyetleri, dolandırıcılık veya kripto varlık hırsızlığıyla bağlantılı olduğu belirtilen fonları komisyon karşılığında kabul ederek dönüştürdüğü ileri sürülmüştür. Soruşturmadaki önemli gelişmelerden biri, 15 Eylül 2025 tarihinde AudiA6 bağlantılı aklama faaliyetlerine katıldığı değerlendirilen Ukrayna uyruklu bir kişinin yakalanması olmuştur. Yakalama sırasında ele geçirilen elektronik cihazların incelenmesi, ağ içerisindeki diğer kişilerin, iletişimlerin ve operasyonel bağlantıların belirlenmesine katkı sağlamıştır.

Soruşturmanın bu aşaması, gizli soruşturma yöntemlerinin elektronik cihaz ve iletişim verilerinin süratle incelenmesiyle desteklenmesinin önemini ortaya koymaktadır. Siber araçlarla gerçekleştirilen karmaşık finansal suçlarda, tek bir şüpheliden elde edilen dijital deliller dahi ağ içerisindeki diğer kişilerin, kullanılan altyapının ve finansal bağlantıların tespit edilmesini sağlayabilmektedir.

III. Koordineli Müdahale ve Malvarlığının Güvence Altına Alınması

Polonya Merkezi Siber Suçlarla Mücadele Bürosu tarafından yürütülen soruşturmanın ardından, Łódź Bölge Savcılığı tarafından yayımlanan kırmızı difüzyon bildirimi temelinde Gürcistan'da yakalama işlemleri gerçekleştirilmiştir.

2 Haziran 2026 tarihli suç duyurusunda Igorevich Tkachuk ve Alexander Vladimirovich Ledenev, AudiA6'nın üst düzey üyeleri ve Dark2Web'in işletmecileri olarak gösterilmiştir. Her iki şüpheli 10 Haziran 2026 tarihinde Gürcistan'da yakalanmış; AudiA6 ve Dark2Web ile bağlantılı dijital altyapı da aynı operasyon kapsamında hedef alınmıştır.

Operasyon sonucunda:

- 25 alan adı kapatılmış;
- 30'dan fazla sunucuya el konulmuş;
- Gürcistan'da 80'in üzerinde araç ile çeşitli taşınmazlar güvence altına alınmış;
- 692.000 avro tutarında kripto varlık dondurulmuş ve
- 86.000 avronun üzerinde ilave kripto varlığa el konulmuştur.

Şüphelilerin, dijital altyapının ve malvarlığı değerlerinin eş zamanlı biçimde hedef alınması operasyonun temel unsurlarından birini oluşturmuştur. Bu yaklaşım; ağ üyelerinin sunucuları başka ülkelere taşıması, delilleri ortadan kaldırması, fonları alternatif cüzdanlara aktarması veya yeni alan adları ve hesaplar üzerinden faaliyetlerini sürdürmesi riskini azaltmıştır.

AudiA6 vakası, müdahale tedbirlerinin koordineli şekilde planlanması ve uygulanması gerektiğini ortaya koymaktadır. Kripto varlık bağlantılı soruşturmalarda yakalama işlemleri; ilgili cihazların, sunucuların, alan adlarının, hesapların ve malvarlığı değerlerinin gecikmeksizin güvence altına alınmasıyla desteklenmediği takdirde beklenen sonucu vermeyebilir.

IV. Müşterini Tanı *(KYC)* Kayıtları, Dijital Altyapı ve Soruşturma Göstergeleri

Soruşturma kapsamında, AudiA6 ağıyla bağlantılı olarak kullanıldığı değerlendirilen hesaplara ilişkin 6.000'den fazla müşterini tanı (**"KYC"**) kaydı tespit edilmiştir. Bu hesapların önemli bir bölümünün, suç gelirlerini yasal kripto varlık alım satım platformları üzerinden aktarmak amacıyla kullanılan Rusça konuşan aracılarla bağlantılı olduğu belirtilmektedir.

Hesapların, ticari e-posta sağlayıcıları ile organizasyonun kontrolündeki alan adlarına bağlı e-posta adresleri kullanılarak oluşturulduğu tespit edilmiştir. İlgili alan adları, kripto varlık hizmet sağlayıcılarının aklama ağıyla bağlantılı olabilecek hesapları tespit etmesine ve engellemesine yardımcı olmak amacıyla kamuya açıklanmıştır.

Bu bulgular, kripto varlık aklama soruşturmalarının yalnızca blokzincir verileriyle sınırlı yürütülmemesi gerektiğini göstermektedir. Blokzincir analizi fonların hareketlerini ortaya koyabilse de ilgili cüzdan veya hesapları fiilen kontrol eden kişileri tek başına göstermeyebilir.

KYC kayıtları, kripto varlık platformlarındaki hesap bilgileri, e-posta adresleri, alan adı kayıtları, cihaz verileri ve iletişim kayıtları; blokzincir üzerindeki işlemlerin belirli kişi veya organizasyonlarla ilişkilendirilmesinde belirleyici rol oynayabilir. Bu verilerin birlikte incelenmesi, aklama ağının operasyonel yapısının, kullanılan aracıların ve suçtan kaynaklanan fonların yasal platformlara giriş yaptığı veya bu platformlar üzerinden aktarıldığı noktaların tespit edilmesini sağlayabilir.

V. AudiA6 Operasyonunun Arkasındaki Uluslararası İş Birliği

AudiA6 soruşturması, bir tarafta Amerika Birleşik Devletleri Gizli Servisi ve Amerikan Gelir İdaresi Ceza Soruşturmaları Birimi, diğer tarafta ise Polonya Polisi tarafından yürütülen paralel soruşturmaları kapsamıştır. Europol, Eurojust ve diğer uluslararası kolluk makamları soruşturma ve operasyon sürecine destek sağlamıştır.

Eurojust; Fransa, Polonya, Gürcistan ve İzlanda'yı ilgilendiren adli tedbirleri koordine etmiştir. Amerika Birleşik Devletleri, Gürcistan ve İzlanda'dan irtibat savcıları da sürece katkıda bulunmuştur. Amerika Birleşik Devletleri, Fransa, Polonya, Gürcistan, Almanya, İzlanda, Japonya, İsviçre, Birleşik Krallık, Kanada ve Avustralya makamları operasyona veya bağlantılı soruşturmalara katılmıştır. Bu kapsamlı iş birliği, kripto varlık aklama faaliyetlerinin sınır ötesi niteliğini ortaya koymaktadır. Söz konusu soruşturmalarda şüpheliler, dijital altyapı, hizmet sağlayıcılar, hesaplar ve malvarlığı değerleri çoğu zaman farklı ülkelerde bulunmaktadır. Bu nedenle tek bir ülke makamının, ağın bütünüyle ortaya çıkarılması için gerekli bütün delillere veya tedbir yetkilerine sahip olması mümkün olmayabilir.

AudiA6 operasyonu; paralel soruşturmaların, hızlı bilgi paylaşımının, koordineli adli tedbirlerin ve yetkili makamlar arasında sürekli iletişimin uygulamadaki önemini göstermektedir. Bu mekanizmalar, sınır ötesinde bulunan şüpheli ve malvarlığı unsurlarının tespitini, operasyonların eş zamanlı yürütülmesini ve deliller ile suç gelirlerinin resmî tedbirler uygulanmadan önce başka ülkelere aktarılması riskinin azaltılmasını sağlamaktadır.

VI. Kripto Varlık Soruşturmaları Bakımından Temel Çıkarımlar

AudiA6 vakası, karmaşık kripto varlık aklama soruşturmalarında blokzincir üzerindeki işlemlerin izlenmesinin gerekli olmakla birlikte tek başına yeterli olmadığını göstermektedir. Etkili bir soruşturma stratejisinde blokzincir analizinin; i) gizli soruşturma faaliyetleri, ii) KYC ve kripto varlık platformu kayıtları, iii) elektronik cihaz incelemeleri, iv) alan adı ve sunucu verileri, v) e-posta ve iletişim kayıtları, vi) finansal istihbarat verileri ve vii) geleneksel malvarlığı araştırma yöntemleriyle birlikte yürütülmesi gerekmektedir.

Vaka ayrıca, aklama ağının yalnızca belirli üyelerine değil, bütün operasyonel yapısına müdahale edilmesi gerektiğini ortaya koymaktadır. İlgili sunucular, alan adları, cüzdanlar, hesaplar ve malvarlığı değerleri eş zamanlı olarak güvence altına alınmadan yalnızca şüphelilerin yakalanması; ağın diğer üyelerinin faaliyetlerine devam etmesine, delilleri ortadan kaldırmasına veya suç gelirlerini başka ülke ve cüzdanlara aktarmasına imkân sağlayabilir. Bunun yanında alan adları, hesap bağlantıları ve diğer teknik göstergelerin kamuya açıklanması, kripto varlık hizmet sağlayıcılarının bağlantılı faaliyetleri tespit etmesine ve uygun risk temelli tedbirleri uygulamasına katkı sağlayabilir. Nihayetinde AudiA6 operasyonu; paralel soruşturmaların, hızlı bilgi paylaşımının, koordineli adli tedbirlerin ve sınır ötesi malvarlığı araştırmalarının şüphelilerin tespit edilmesi, dijital altyapının devre dışı bırakılması ve suç gelirlerinin dondurulması veya bunlara el konulması ihtimalini önemli ölçüde artırdığını göstermektedir.