



İKV BİLGİ NOTU

AB CİDDİ VE ORGANİZE SUÇ TEHDİT DEĞERLENDİRMESİ 2025 RAPORU

Hatice Zeynep Şen, İKV Uzman Yardımcısı

Avrupa Polis Teşkilatı *Europol*, 18 Mart 2025 tarihinde AB Ciddi ve Organize Suç Tehdit Değerlendirmesi (*EU Serious and Organised Crime Threat Assessment-EU-SOCTA*) 2025 raporunu yayımladı.¹ EU-SOCTA, ciddi ve organize suçların AB'nin iç güvenliğine yönelik oluşturduğu tehditler hakkında yürütülen en kapsamlı analizlerden bir olarak ön plana çıkıyor. AB Üye Devletleri ve uluslararası kolluk kuvvetleri ortaklarından alınan istihbarata dayanan rapor, yalnızca organize suçun bugünkü durumunu analiz etmiyor, aynı zamanda yarının tehditlerini de öngörerek Avrupa'nın kolluk kuvvetleri ve politika yapıcılarına sürekli gelişen organize suçun önüne geçebilmeleri için bir yol haritası sunuyor. Rapora göre Avrupa genelinde siber suçlar, uyuşturucu ticareti, insan kaçakçılığı, kara para aklama ve çevre suçlarının yükselişte olduğu ifade ediliyor. Ek olarak suç örgütlerinin yalnızca yasa dışı faaliyetler yürütmekle kalmadığı aynı zamanda AB'nin ekonomik, siyasi ve sosyal yapısını giderek zayıflattığı ifade ediliyor.

Organize Suçun Yöntemleri

Organize suçun kullandığı yöntemler arasında kara para aklama, sahte şirketler üzerinden eylemler, yolsuzluk ve rüşvet, organize şiddet ve gençlerin suça sürüklenmesi yer alıyor. Organize suç grupları kazançlarını yasallaştırmak ve yasa dışı faaliyetlerini gizlemek için dijital varlıklar üzerinden kara para aklama, örtülü finansal sistemleri yoluyla gizli işlemler gerçekleştirme, finans sektöründe yasadışı fonları dolaşıma sokma ve sahte şirketlerin kullanılması gibi yöntemleri kullanıyor. Özellikle lojistik, inşaat ve gayrimenkul sektörleri organize suç örgütlerinin en çok kullandığı sektörler. Kripto para ve *fintech* sistemlerinin de rüşvet ve yolsuzluğu gizlemek için kullanıldığı ifade ediliyor. Suç örgütlerinin şiddet kullanımını giderek arttırdığı ve özellikle gençleri şiddet eylemlerine yönlendirmek için sosyal medyayı kullandıkları belirtiliyor. Sosyal medya ve oyun platformları gibi alanların gençlerin suç gruplarına katılımını kolaylaştırdığı da vurgulanıyor.

2025 Raporunda Öne Çıkan Tehditler ve Organize Suçun Değişen "DNA'sı"

Europol 2025 raporunda suç ağlarının daha karmaşık ve tehlikeli hale geldiği yedi temel alan vurgulanıyor. Bunlar;

1. Siber Saldırıları
2. Çevrim içi Dolandırıcılık
3. Çevrim içi Çocuk Cinsel İstismarı
4. Göçmen Kaçakçılığı
5. Uyuşturucu Kaçakçılığı

¹ Europol, "2025 EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT", 18.03.2025, <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>



6. Ateşli Silah Kaçakçılığı

7. Çevresel Atık Suçları

Rapordaki en önemli vurgu, organize suçun “DNA’sının” yapay zekâ ve yeni teknolojiler gibi nedenlerle temelden değiştiği ve her zamankinden daha yerleşik ve daha istikrarsız hale geldiği. Rapor, organize suç örgütlerinin, yapay zekâ, *blockchain* ve diğer dijital araçları kullanarak faaliyetlerini genişlettiği ve bunların tespit ve önlenmesinin giderek zorlaştığı konusunda uyarıda bulunuyor. Ayrıca uyuşturucu ticaretinden insan kaçakçılığına kadar birçok suç faaliyetinin online platformlara taşındığı, suç örgütlerinin bu dijital dünyayı, faaliyetlerini genişletmek ve izlerini gizlemek için aktif olarak kullandığı belirtiliyor. Özellikle kara para aklama yöntemi olarak kripto paraların kullanımı ön plana çıkıyor. Çevrim içi ortamda artan suçlar arasında, sahte yatırım seçenekleri ve ponzi sistemleriyle milyonlarca avro haksız kazanç elde edilmesi, kurumsal e-posta dolandırıcılığı ile şirketlerin hedef alınması ve çevrim içi uyuşturucu ve yasa dışı mal ticaretinin hızla büyümesi yer alıyor. Suç örgütlerinin kara para aklamak için kripto para borsaları ve merkeziyetsiz finans (*DeFi*) sistemlerinin yanı sıra özel jetonlar ve NFT’ler gibi yeni teknolojileri de kullandığına dikkat çekiliyor. Çevrim içi ortamda artan bir diğer suç türü ise çevrim içi çocuk istismarı ve cinsel suçlar. Yapay zekâ ile çocuk istismarına yönelik materyallerin üretiminin ve paylaşımının arttığı ve yeni şifreleme teknolojilerinin bu suçların tespit edilmesini zorlaştırdığına dikkat çekiliyor. Ayrıca çocukların çevrim içi ortamda hedef alınarak suç örgütleri tarafından istismar edilmesinin yaygınlaştığı da belirtiliyor. Bir diğer suç türü ise sosyal medya üzerinden yapılan dezenformasyon kampanyaları. Bunların toplumu içten zayıflatma riski taşıdığı belirtiliyor. Bunlar dışında belli gruplara silah sağlayarak yasal engellerin aşılması, yaptırımların çeşitli yollarla delinmesi, altyapı sabotajları, kundaklama ve kaçırma gibi eylemlerin de hibrit tehditleri beslediğine dikkat çekiliyor. Bunların tespitinin ve önlenmesinin giderek zorlaştığı da ifade ediliyor.

Yeni Teknolojilerle Hızlanan Suçlar

Raporda yapay zekânın ve diğer ileri teknolojilerin organize suçlar için yeni fırsatlar yarattığı belirtiliyor. Bunlardan ilki yapay zekâ destekli dolandırıcılık ve manipülasyon. Bunun yöntemleri arasında ses ve görüntü taklitleriyle (*deepfake*) dolandırıcılık ve yapay zekâ destekli kimlik sahtekarlığı ile banka ve finans sistemlerinin hedef alınması yer alıyor. Kara para aklama, yasadışı finans suçlarında ise kripto para ve *blockchain* teknolojisi gibi yeni yöntemler sayesinde finansal işlemlerin suç örgütleri tarafından daha anonim hale getirilebildiği belirtiliyor. Ek olarak sahte para basımı ve dijital varlık hırsızlığının da artış gösterdiği ifade ediliyor. Siber saldırıların yapay zekâ ile şirket ve kamu kurumlarının veri güvenliğini daha fazla tehdit etmeye başladığı belirtiliyor. Yapay zekânın suçluların daha az kaynakla daha fazla kurbanı ulaşmasını, hedefe yönelik hareket edebilmesini ve küresel erişimlerini genişlettiğine dikkat çekiliyor. Dahası tamamen otonom yapay zekâ ortaya çıkarsa eğer baştan sona yapay zekâ kontrollü suç ağlarının önünü açarak, organize suçlarda yeni bir döneme işaret edebileceğine vurgu yapılıyor. Çünkü bu suç şebekelerinin giderek daha güçlü hale gelen geniş bir yetenek



yelpazesine ulaşması anlamına geliyor. Mevcutta suçluların CCTV gözetimi, çipler, dronlar, GPS ve 3D baskı gibi araçları kendi avantajlarına çevirdikleri ifade ediliyor. Yeni teknolojilerin daha da gelişmesiyle birlikte suç şebekelerinin şu anda sergilediği yüksek düzeyde anonimlik, hız ve karmaşıklığın önümüzdeki yıllarda muhtemelen daha da artacağına vurgu yapılıyor. Hatta burada suç örgütlerinin kullandığı “şimdi sakla, sonra şifresini çöz” (*Store Now, Decrypt Later*) denen bir yaklaşımdan da bahsediliyor. Bu yaklaşım daha gelişmiş hesaplama yetenekleri kullanılabilir hale geldiğinde, şifresini daha sonra çözmek amacıyla mevcutta şifrelenmiş verilerin toplanmasını ve depolanmasını içeriyor. Bu tür uygulamaların mevcut şifreleme standartlarını geçersiz kılma tehdidi oluşturduğundan hükümetlerin, işletmelerin ve vatandaşların hassas bilgileri için önemli bir risk oluşturduğuna dikkat çekiliyor.

Öneriler

Raporda genel olarak AB ve Üye Devletler, kanun yapıcılar ve kolluk kuvvetleri arasında iş birliğinin artırılması gerektiği belirtiliyor. Özellikle hukuki düzenlemelerin yapay zekâ ve kripto paralar gibi yeni teknolojilere daha fazla uyumlu hale getirilmesi gerektiği ifade ediliyor. Mevcut durumda yalnızca %2'sine el konulabilen suç gelirleri ile daha etkin mücadele edilmesi gerektiği ve finansal kaynakların hedef alınarak organize suçların ekonomik güçlerinin zayıflatılması gerektiği belirtiliyor. Gençlerin suç faaliyetlerine yönlendirilmesinin engellemesi için daha sıkı sosyal medya denetimlerine de işaret ediliyor. Siber güvenlik önlemlerinin sıkılaştırılması önerisini de içeren rapor, tüm bu süreçlerde hem uluslararası iş birliğinin geliştirilmesi hem de *Europol*'ün bu mücadelede merkezi rol oynaması gerektiğini vurguluyor.