

# Bilişim Çağının Kriminal Örgütleri: "e-mafya"

## Çığır İlbaş

cigir@baskent.edu.tr

Başkent Üniversitesi, İktisadi ve İdari Bilimler Fakültesi

Bilgisayar ve İnternet teknolojisinin hızlı gelişimi sonucu oluşan e-dünya düzeninin kendine özgü etik değerleri ve normları da hızla şekillenmektedir. Gündelik yaşantımızda, endüstriyel alanlarda ve ulusal boyutlarda birçok avantaja olanak sağlayan bu hızlı gelişim, sosyal ve teknolojik yönden dengesiz değişimleri ve tehditleri de beraberinde getirmektedir.

Fiziksel dünyadaki birçok olgu ve oluşum, e-dünya'da farklı orijin ve ölçeklerde karşımıza çıkabilmektedir. Gelecek yıllarda İnternet Fiziği, İnternet Sosyolojisi, psikolojisi, hukuku, ekonomisi gibi yeni disiplinleri oluşturacak kadar güçlü değişimlerin sonuçlarından bir tanesi ve belki de en tehlikelisi "e-mafya" olarak nitelendirebileceğimiz illegal yazılım, yöntem ve teknikleri örgütsel misyonları doğrultusunda kullanan gruplardır. 1980'li yıllarda Avrupa'da ortaya çıkan bu akımın değişen koşullarla birlikte 1990'lı yıllarda etkinliği azalmıştı. 2000'li yıllarda ise, farklı formlarda doğu ülkelerinde odaklaşıp global bir tehdit haline gelmeye başladı.

Özellikle Rusya, Doğu Avrupa ve Uzakdoğu'da odaklanan hacker, cracker grupları belirli bir örgütsel hiyerarşi ve çalışma sistemi çerçevesinde para karşılığı dijital bilgi çalma, bozma gibi faaliyetler yürütmeye başladılar. Bazı gruplar üniversite veritabanlarında not değişikliği, eş ya da sevgililerin netteki özel hayatının kontrol ve takibi gibi "iş"leri, önceden belirlenmiş fiyat tarifeleri ile garantili olarak gerçekleştirme vaadinde bulunmaktadırlar.

Bu gelişmeler birbiriyle ilişkili birkaç soruyu akla getirmektedir. Hangi sosyal ve teknolojik şartlar, bilişim sektöründe böyle bir tampon mekanizmanın oluşmasına olanak sağlamıştır? Hangi etik anlayış çerçevesinde özel hayata saldırı iş olarak tanımlanmaya başlamıştır? Hangi sosyal sınıfa ait insanlar böyle bir işin sahibi durumundadırlar? Bu soruların yanıtlarını bulabilmek için öncelikle bilgisayar dünyasındaki "yaramaz" çocukların davranış ve eğilimlerinin nedenlerine göz atmamız gerekmektedir.

Sekiz bitlik bilgisayarların gündelik hayatımıza yoğun olarak girdiği 80'li yıllarda, oyun yazılımlarının yüksek ücretlerle satılması beraberinde bilgisayar korsanlığını da gündeme getirmişti.

Yeterli bilgi ve beceriye sahip olduğunda ücretsiz çoğaltılabilen yazılımların üreticilerini korumak için gereken ceza ve ticaret yasaları Batı Avrupa'da hızla yenilendi. Ancak Doğu Avrupa ve Asya bu değişime ayak uydurmakta oldukça geciktiler. Yaklaşık yirmi yıllık gecikmeden sonra Türkiye'de uyum sürecinin ilk adımlarının atıldığını görmekteyiz.

1980'li yıllardaki çoğunluğu 4 - 5 kişiden oluşan bu topluluklarda işbölümüne yönelik uzmanlaşma dikkati çekmekteydi. Orjinal programları gruba temin eden "supplier"lar (bu temin genellikle çalma şeklindeydi), programdaki kopyalanmaya karşı güvenlik sistemini bozan "cracker"lar ve kopyalanabilir hale gelen yazılımı diğer gruplara modemle ya da mektupla ulaştıran "swapper"lar.

Genellikle İngiltere ve Almanya orijinli bu gruplar "It's illegal but who cares" felsefesiyle milyonlarca dolarlık bir pazarı çok zaman geçmeden yıkmayı başardılar ve adeta kendi bindikleri dalları kestiler. 80'li yıllarda telif haklarını koruyan yasaları olmayan Türkiye'de, bu tarz uğraşların ticari değeri yoktu. Zira bütün şehirlerin bulvarlarında en az iki üç "yetkili servis", korsan yazılımları faturayla ve tamamen yasal olarak satabilmekteydi.

1990'lı yıllarda İnternet'in kişisel bilgisayarlara entegre olmasıyla söz konusu gruplar hızla dağıldılar. Orjinal programlar deneme sürümleriyle internette mevcut olduğu için supplier'lara gerek kalmamıştı. Deneme sürümü üzerinde yapılan crack işleminden sonra mektuba ya da modeme gerek kalmadan web teknolojisi sayesinde onbinlerce kişiye ulaşmak mümkün hale gelmişti. Artık yalnızca cracker'lar bu illegal işi üstlenmişti. Korsan gruplarda ise işbölümü ve uzmanlaşmaya yönelik değil yardımlaşmaya ve işi paylaşmaya yönelik kadrolaşmalar oluşmaya başladı. Gruplar dağıldıktan sonra webin arka sokaklarında yaşayan çocuklar, sinema, medya ve basın izlediği yanlış politikalar sonucunda birer kahraman gibi gösterilip gururla bulvarlarda dolaşmaya başladılar.

Diğer taraftan dünyanın doğu yakasında bilgisayar teknolojisini ileri seviyede kullanabilen kişilerin uygun işlerde istihdam edilememesi ve ekonomik çöküntüler nedeniyle birçok programcı ve network uzmanı, İnternet'in karanlık yüzüne doğru yönelmeye başladı. Bu yönelim günümüzde veri güvenliğini "fatal" boyutlarda tehdit eden bir olgu haline geldi.

Entegre ve interaktif sistemlerin yaygınlaşmasıyla virüs, trojan, worm scriptlerini üretme kolaylığı, bilişim dünyasının yeraltı çocuklarını güçlendirmeye ve birleştirmeye devam ediyor. Özellikle 2003 yılının önceki yıllara göre bilişim suçları açısından çok hareketli geçeceği, konunun uzmanlarının ortak görüşü. Bilişim teknolojisindeki gelişmelerin kademeli olarak yaygınlaştırılması, kurumsal destek ve denetimlerin güçlendirilmesi ve sistemde kilit nokta olan "insan" faktörünün de aynı paralellikte geliştirilmesi şartları sağlanamazsa, tehditlerin teknolojinin önünü kesmesi kaçınılmaz bir son olarak karşımıza çıkabilir.