DİJİTAL DÖNÜŞÜM VE SİBER GÜVENLİK DERNEĞİ

DEĞERLENDİRME YAZISI

www.ddsgd.org

17,1 Milyon Uyarı: Türkiye Siber Tehdit Haritasının Neden Zirvesinde?

Kaspersky META Bölgesi Raporu, Ertelenemez Bir Uyarı Niteliği Taşıyor

Rakamlar acı bir gerçeği gözler önüne seriyor. Kaspersky'nin Orta Doğu, Türkiye ve Afrika (META) bölgesine ilişkin son tehdit değerlendirmesi, Türkiye'yi kayıtsız kalınamayacak bir tablonun tam ortasına yerleştiriyor. 2026'nın ilk yarısında, **Türkiye web tabanlı tehditlerden en yüksek oranda etkilenen ülke oldu** ve yalnızca bu dönemde ülkemizde 17,1 milyon çevrim içi saldırı engellendi. Bu, bir başarı hikâyesi değil; ciddiyetle ele alınması gereken bir alarmdır.

Dijital Dönüşüm ve Siber Güvenlik Derneği olarak, bu tablonun yarattığı riskleri hafife alma lüksümüz olmadığına inanıyoruz. Bu değerlendirmede, raporun ortaya koyduğu tehditleri eleştirel bir gözle ele alıyor ve neden acil bir farkındalık ve hazırlık gerektiğini ortaya koyuyoruz.

Türkiye Neden Bölgenin En Çok Hedef Alınan Ülkesi?

Raporun en çarpıcı bulgusu, Türkiye'nin web kaynaklı saldırılardan etkilenen kullanıcı oranında **yüzde 26,8** ile bölge lideri olmasıdır. Ülkemizi yüzde 21,2 ile Kenya ve yüzde 19,3 ile Katar takip ediyor. Bu sıralama tesadüf değil; Türkiye'nin dijitalleşme hızı, genç ve yoğun internet nüfusu ve stratejik konumu, onu hem sıradan siber suçlular hem de devlet destekli gruplar için cazip bir hedef hâline getiriyor.

Bu veriler, ülkemizin dijital savunma kapasitesini artırmasının artık bir tercih değil, bir **zorunluluk** olduğunu açıkça gösteriyor. Engellenen saldırı sayısının yüksekliği kadar, saldırıların yoğunluğu ve sürekliliği de kaygı verici bir tablo çiziyor.

Yapay Zekâ: Saldırganların Elindeki En Tehlikeli Silah

Raporun altını çizdiği en kritik uyarı, yapay zekânın artık saldırganların hizmetinde olduğudur. Kaspersky uzmanı Sergey Lozhkin'in ifadesiyle, yapay zekâ; zararlı araçların geliştirilmesi ve uyarlanması için gereken süreyi ve maliyeti azaltarak, tehdit aktörlerinin çok daha hızlı ve geniş ölçekte hareket etmesine olanak tanıyor. Bu, savunmacılar için tehlikeli bir asimetri yaratıyor.

Raporda dikkat çekilen yeni nesil tehdit eğilimleri özellikle endişe verici:

- **Yapay zekâ destekli zararlı yazılımların evrimi:** Üretken YZ modelleri, zararlı yazılımların farklı programlama dillerine ve sistem mimarilerine kolayca uyarlanmasını sağlıyor; bu da tespiti zorlaştırıp yayılmayı hızlandırıyor.

- **Otonom yapay zekâ ajanları:** Üretken araçların otonom işlem yapabilen ajanlara dönüşmesi, işletmeler için tamamen yeni bir saldırı yüzeyi açıyor.
- **Bulut tabanlı veri sızdırma:** Saldırganlar, çalınan verileri meşru bulut ve dosya paylaşım hizmetleri üzerinden aktararak normal ağ trafiği içinde gizleniyor.
- **Operasyonları hedef alan fidye yazılımları:** Bazı gruplar artık yalnızca veriyi şifrelemekle kalmıyor; üretim ve iş süreçlerini de durdurarak fidye baskısını artırıyor.

Görünmez Tehlike: APT Grupları ve Siber Casusluk

Belki de en sinsi tehdit, gelişmiş kalıcı tehdit (APT) gruplarından geliyor. Rapora göre **Kaspersky, 2026 itibarıyla META bölgesindeki kuruluşları aktif olarak hedef alan 20'den fazla APT grubunu takip ediyor.** Bu gruplar artık yalnızca sistemlere sızmayı değil, mümkün olduğunca uzun süre fark edilmeden ağ içinde kalmayı hedefliyor.

Uzmanların vurguladığı üzere, saldırganlar hassas projelere, kurumsal belgelere, e-posta hesaplarına ve kimlik bilgilerine erişim sağlamaya odaklanıyor. Jeopolitik gerilimlerin bu saldırıların temel itici gücü olması, kamu kurumları ve kritik altyapılar açısından riski daha da büyütüyor. MuddyWater gibi grupların bölgede daha önce görülmemiş zararlı yazılım zincirleri kullanması, tehdidin ne denli evrildiğinin somut bir kanıtıdır.

İki Ucu Keskin Bıçak: Kurumların Yapay Zekâ Telaşı

Rapordaki bir başka çarpıcı bulgu, kurumların bu tehdit ortamına hazırlık düzeyiyle ilgili. Kaspersky'nin 18 ülkeden 1.800 bilişim ve siber güvenlik karar vericisiyle yaptığı araştırma, yapay zekâ entegrasyonunun kurumlar genelinde hızla yayıldığını ortaya koyuyor. Ancak burada kritik bir uyarı gizli: Yapay zekâyı hızla benimseyen kurumların, bu süreci **güçlü güvenlik çözümleri, net prosedürler ve kapsamlı eğitimlerle** desteklemesi şart.

Aksi hâlde, verimlilik uğruna aceleyle devreye alınan yapay zekâ araçları, kurumların bizzat kendi elleriyle açtığı yeni güvenlik açıklarına dönüşebilir. Teknolojiyi benimseme hızının, onu güvenli kılma hızını geçmesi, en büyük risklerden biridir.

Sonuç: Farkındalık Bir Tercih Değil, Zorunluluktur

Kaspersky'nin verileri, üzerinde düşünülmesi gereken güçlü bir uyarı niteliği taşıyor. Türkiye, dijitalleşmenin nimetlerinden yararlanırken, aynı zamanda bu sürecin getirdiği risklerin de en yoğun yaşandığı ülkelerden biri konumundadır. Bu gerçeği görmezden gelmek, telafisi güç sonuçlar doğurabilir.

Dijital Dönüşüm ve Siber Güvenlik Derneği olarak çağrımız nettir: Kurumlarımız, siber güvenliği bir maliyet kalemi olarak değil, varlıklarının teminatı olarak görmelidir. Yapay zekâ araçları güvenlik önlemleriyle birlikte devreye alınmalı, çalışan farkındalığı sürekli canlı tutulmalı ve kritik altyapılar öncelikli olarak korunmalıdır. Bu tehdit ortamında en büyük zafiyet, tehlikenin farkında olmamaktır. Derneğimiz, bu farkındalığın artırılması ve nitelikli savunma kapasitesinin geliştirilmesi için üzerine düşeni yapmaya kararlıdır.

Yararlanılan Kaynaklar

Anadolu Ajansı (AA) – "Kaspersky META bölgesinin siber tehdit görünümünü açıkladı"

Yeni Çağrı Gazetesi / AA – "Kaspersky, siber casusluk ve yapay zeka kaynaklı riskleri 'Siber Güvenlik Hafta Sonu'nda değerlendirdi"

Donanım Haber – "Kaspersky, 2026'nın ilk yarısında META bölgesini şekillendiren siber tehditleri ortaya koydu"

Fuar Dergisi – "Kaspersky, META Bölgesinin Siber Tehdit Haritasını Açıkladı"

Haberler.com – "Kaspersky'den Tiflis'te Siber Güvenlik Zirvesi"

Patron Rehberi – "Kritik Tehdit Türkiye'de Hız Kesmedi" ve "Yapay Zeka Riskinde Kritik Gelişme"

Not: Raporun tam metnine ve güncel verilere Kaspersky'nin resmî kaynaklarından ulaşılabilir.

Taner Çıtak

Dijital Dönüşüm ve Siber Güvenlik Derneği Başkanı

www.ddsgd.org

Bu değerlendirme yazısı, Kaspersky'nin META (Orta Doğu, Türkiye ve Afrika) bölgesine yönelik 'Siber Güvenlik Hafta Sonu' etkinliğinde paylaşılan tehdit değerlendirmesine ilişkin kamuya açık basın haberleri temel alınarak hazırlanmıştır. Aktarılan istatistikler ilgili haberlerde yer aldığı biçimiyle kullanılmıştır.