İstanbul Senin Hacklendi mi?

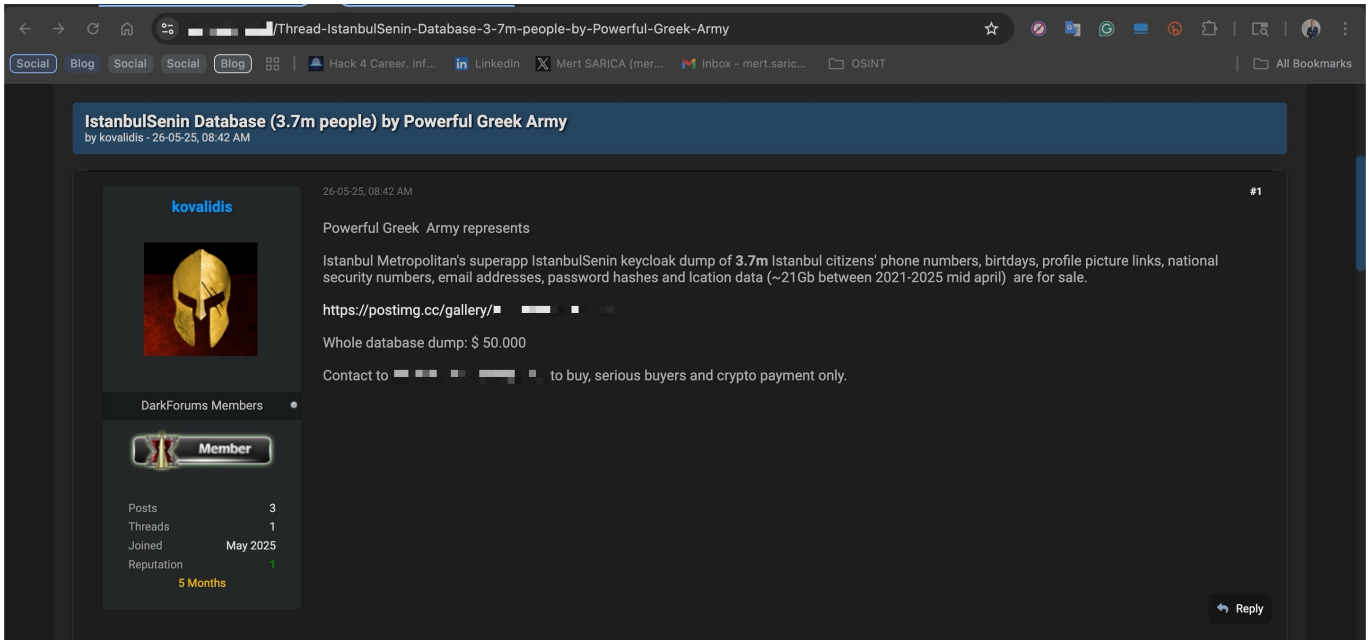
written by Mert SARICA | 6 November 2025
If you are looking for an English version of this article, please visit here.

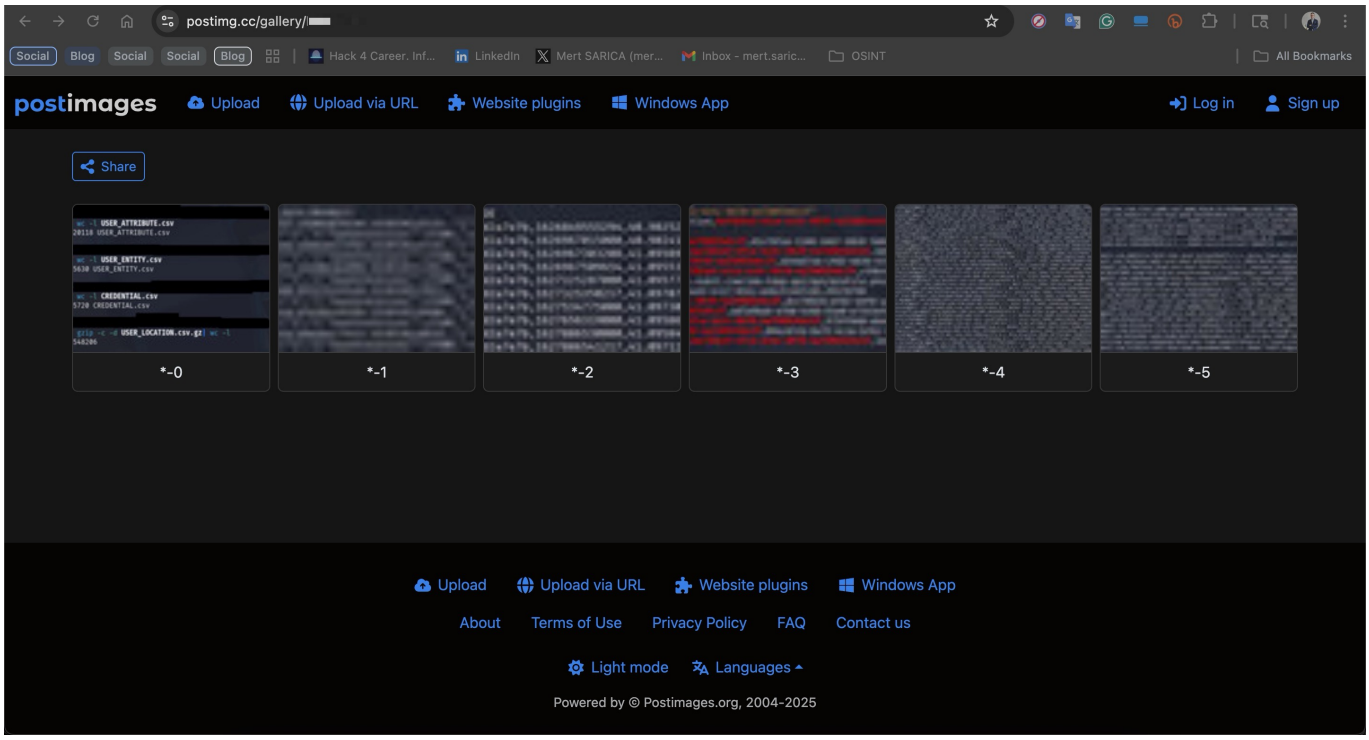
İÇİNDEKİLER

Başlangıç

Tarihler 26 Mayıs 2025 tarihini gösterdiğinde, siber suçluların boy gösterdiği DarkForums isimli platformda kovalidis isimli tehdit aktörü tarafından bir mesaj paylaşıldı. Bu mesajda Powerful Greek Army (PGA) hacker grubunun üyesi olan veya süsü verilen tehdit aktörü, 3.7 milyon Türk vatandaşına ait bilgileri içeren İstanbul Senin veritabanını 50.000$'a satışa sunduğunu belirtiyordu. Dürüst satıcı imajı çizmek adına mesajında, sızdırılan verilere dair ekran görüntülerine de yer vermeyi ihmal etmemişti.

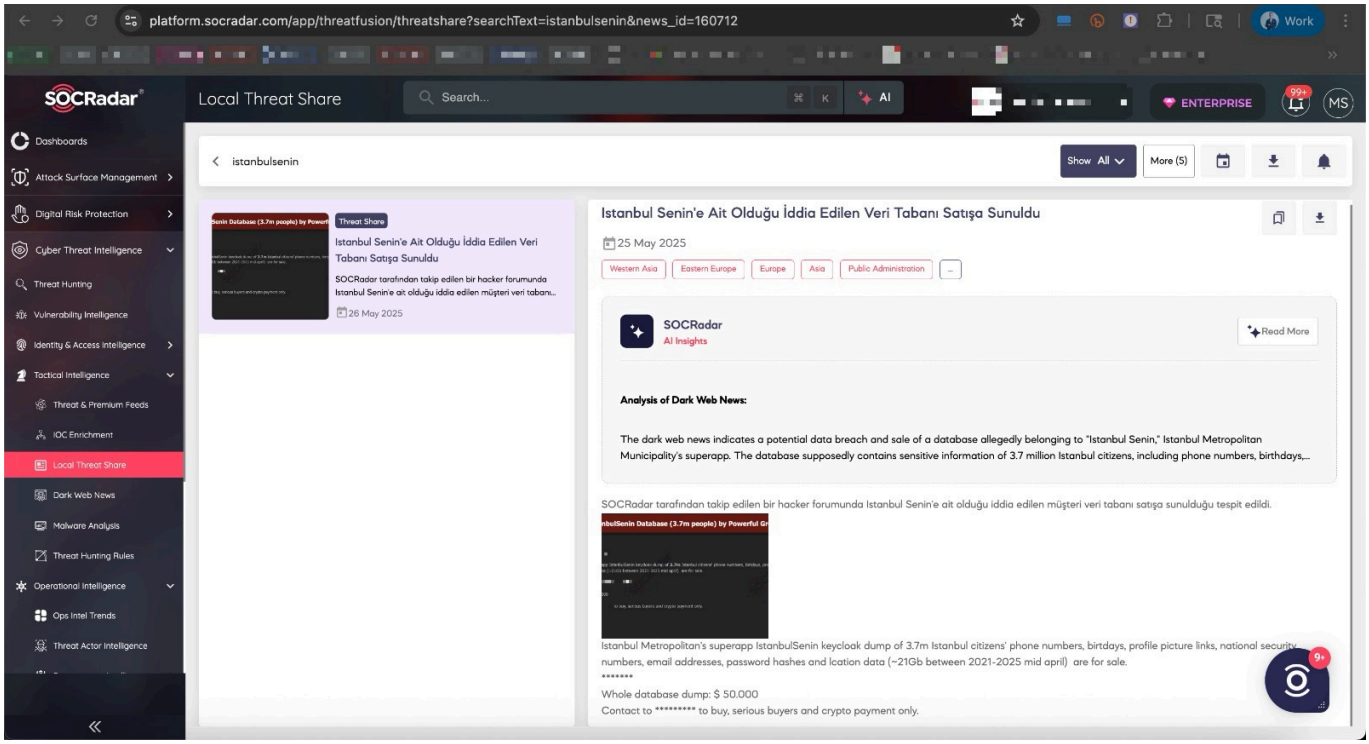
PGA'nın resmi X hesabında bu saldırıya dair bir mesaj paylaşılmamış olması ve tehdit aktörünün DarkForums platformuna sadece bu mesajı paylaşmak için kayıt olması, bunun bir sahte bayrak operasyonu olma ihtimalini akıllara getiriyordu.





İstanbul Senin, İstanbul Büyükşehir Belediyesi'nin şehir yaşamını dijitalleştirmek ve vatandaşlara daha hızlı hizmet sunmak için geliştirdiği yenilikçi bir mobil uygulamadır. Uygulama; toplu taşıma verileri, trafik durumu, otopark bilgileri, kültür-sanat etkinlikleri, spor alanı rezervasyonları, belediye hizmetlerine erişim, ödeme işlemleri ve semtine özel duyurular gibi pek çok özelliği tek çatı altında toplar. Kullanıcılar; İstanbulkart entegrasyonu, çevrimiçi başvurular, randevu sistemleri ve şehir içi avantaj kampanyaları sayesinde günlük ihtiyaçlarını kolayca yönetebilir. İstanbul Senin, şehrin dijital asistanı olmayı hedefleyen, İstanbul'da yaşayan herkesin hayatını kolaylaştıran kapsamlı bir şehir uygulamasıdır.

Bölgesel tehditleri adım adım izleyen SOCRadar Siber Tehdit İstihbaratı Platformu ve bunlara yönelik olarak gönderilen anlık iletiler sayesinde o zamanlar çok sayıda kurum ve kuruluş bu olası sızıntıdan çok kısa sürede haberdar olmuştu.



@MertSARICA incelemeden inanmam

Gel zaman git zaman bu mesajın paylaşılmasının üzerinden yaklaşık 5 ay geçtikten sonra 4 Kasım 2025 tarihinde red.eth rumuzlu bir kullanıcı tarafından X platformu üzerinde etikenlendiğime dair bir uyarı aldım. Etikete konu olan yoruma baktığımda “@MertSARICA incelemeden inanmam” ifadesi hemen dikkatimi çekti. Ana mesaja baktığımda ise Ece SEVİM isimli gazetecinin 5 ay önceye konu olan bu olaya dair bir mesaj paylaştığını gördüm.

Post

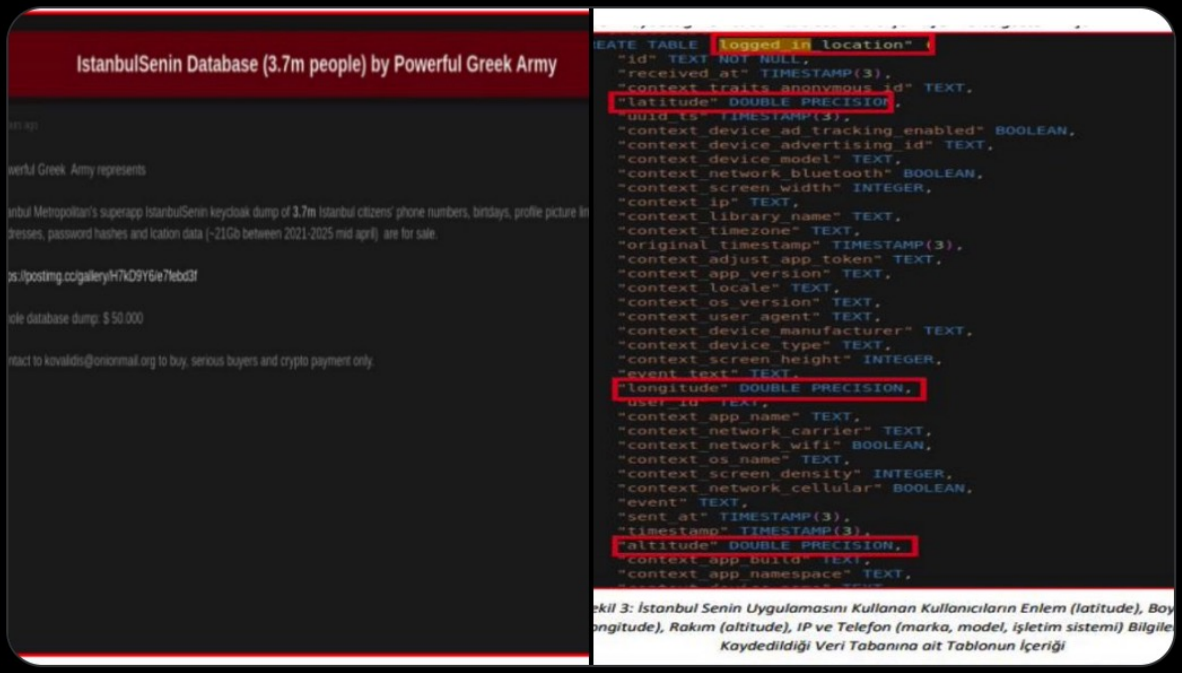
Reply

Ece Sevim @ecesevimtr · Nov 4

DETAY - USOM RAPORU / İBB İSTANBUL SENİN UYGULAMASI VERİLERİNİN DARKWEB'DE 50 BİN DOLAR'A SATIŞI

26 Mayıs 2025 tarihinde, USAM'a İstanbul Senin uygulamasına kaydolan 3.7 milyon vatandaşa ait kimlik (ad, soyad, TCKN), GSM, konum (enlem, boylam) gibi kişisel verilerin

Show more



Kaydedildiği Veri Tabanına ait Tablonun İçeriği

33 168 368 15K

red.eth
@tcctus

@MertSARICA incelemeden inanmam

2:47 PM · Nov 4, 2025 · **421** Views

Clear Web, Deep Web ve Dark Web terimleri son kullanıcılar kadar medya mensupları tarafından da birbirine çok karıştırıldığı için açıklamalarına da yer vermek istedim. Bu açıklamalara istinaden DarkForums'un Dark Web'de yer almadığını rahatlıkla söyleyebiliriz.

Clear Web (Yüzey Web): Arama motorları tarafından indekslenmiş, herkese açık web siteleridir. Kurumsal web sayfaları, haber siteleri, sosyal medya platformları, forumlar bu katmanda yer alır.

Deep Web (Derin Web): Arama motorları tarafından indekslenmeyen, ancak yasal ve güvenli bölümleri de kapsayan alandır. Ücretli veritabanları, akademik arşivler, kimlik doğrulaması gerektiren portallar (örneğin hastane sistemleri, devlet servisleri, özel forumlar) bu kapsamda değerlendirilir.

Dark Web (Karanlık Web): Deep Web'in küçük bir alt kümesidir. Erişim için genellikle Tor veya I2P gibi anonimlik odaklı ağlar kullanılır. Yasadışı pazar yerleri, veri sızıntı forumları, fidye yazılımı operasyonları gibi tehdit istihbaratı açısından kritik kaynaklar burada bulunur.

Türkiye ve hızla değişen gündemine yıllardır uzak olan bir vatandaş olarak, 5 ay aradan sonra DarkForums platformundaki bu tehdit aktörüne ait mesajın neden tekrar gündeme geldiğini pek anlayamadım. Bunu anlamayı bir kenara bırakıp Akıllı Çocuk Saatleri, Instagram Dolandırıcıları, Arka Kapı Avı, Tuzak Sistem ile Hacker Avı vb. blog yazılarında olduğu gibi okurlarına, takipçilerine her daim kulak veren bir siber güvenlik araştırmacısı olarak bu defa red.eth'nin yardım çağrısına yanıt vermeye karar verdim.

Post

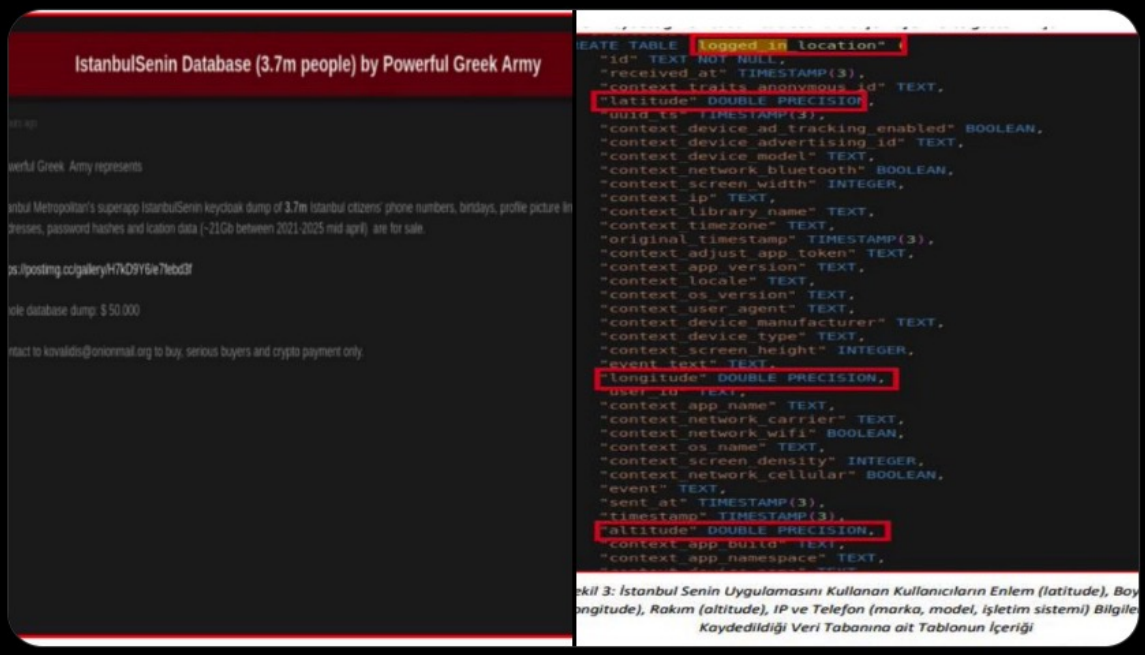
Reply

Ece Sevim @ecesevimtr · Nov 4

DETAY - USOM RAPORU / İBB İSTANBUL SENİN UYGULAMASI VERİLERİNİN DARKWEB'DE 50 BİN DOLAR'A SATIŞI

26 Mayıs 2025 tarihinde, USAM'a İstanbul Senin uygulamasına kaydolan 3.7 milyon vatandaşa ait kimlik (ad, soyad, TCKN), GSM, konum (enlem, boylam) gibi kişisel verilerin

Show more



Kaydedildiği Veri Tabanına ait Tablonun İçeriği

33 168 368 15K

red.eth @tcctus · Nov 4

@MertSARICA incelemeden inanmam

2 430

red.eth
@tcctus

Show translation

@MertSARICA abi inceleyip bi döküman olsa sitede tadından yenmez valla

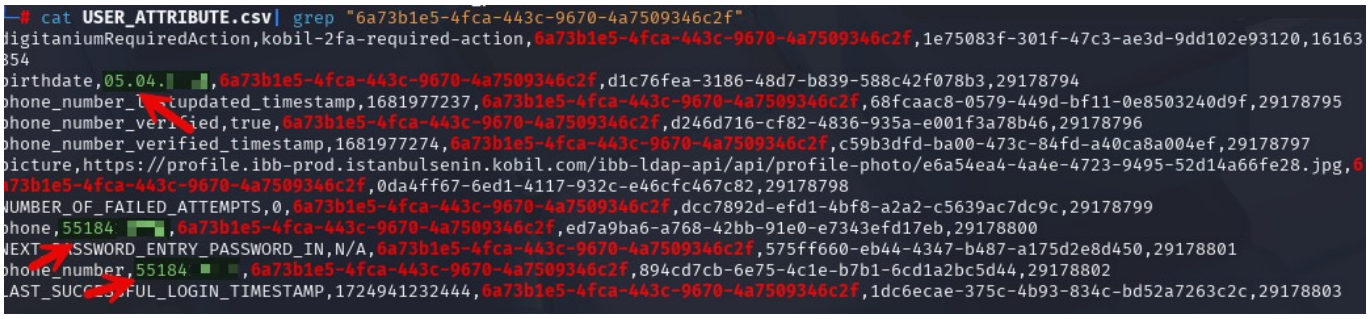
1:44 AM · Nov 5, 2025 · **61** Views

red.eth aslında 50.000$'ı olmayan veya olsa da bunun için harcamak istemeyen

sade bir vatandaş olarak verilerinin çalınıp, çalınmadığını öğrenmek istiyordu. Bu gibi hacklenme ve/veya veri sızıntıları ile ilgili medyada yer alan haberlerde çoğu zaman doğru bilgiye ulaşmak kolay olmadığı için yardım aramaya koyulmuştu. Ben de bu vesileyle sade vatandaş gözüyle bir veri sızıntısının mümkün olan koşullarda, nasıl doğrulanabileceğine dair bir yazı hazırlamaya ve red.eth gibi kişilere yol göstermeye karar verdim.

Nerede Benim Yakın Gözlüğüm? (Analiz)

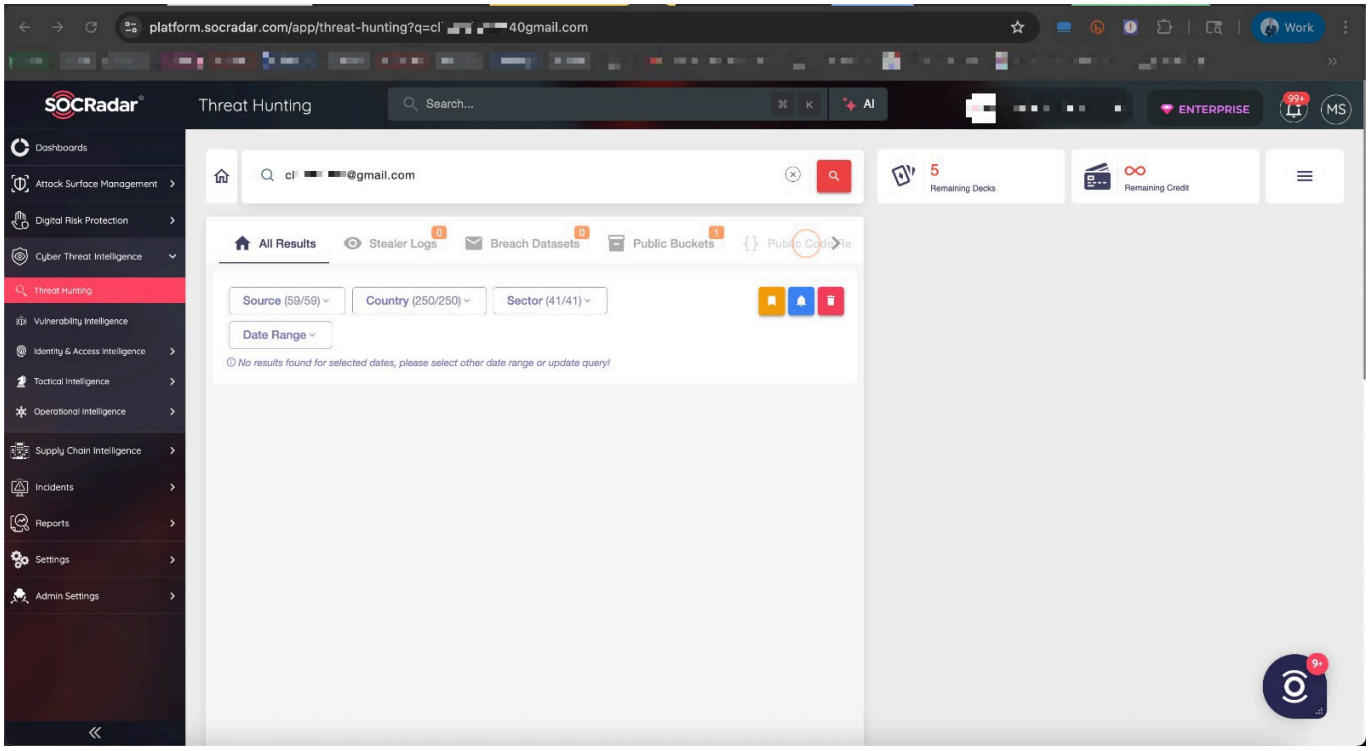
kovalidis isimli tehdit aktörü tarafından paylaşılan örnek verilerin yer aldığı ekran görüntülerin birinde öncelikle kırmızı ile işaretlenmiş UUID / GUID (benzersiz tanımlayıcı) değeri, daha sonra ise sızıntı olayını doğrulamada kullanabileceğim doğum tarihi (05.04.****) ve cep telefonu numarası (055184*****) dikkatimi çekti.

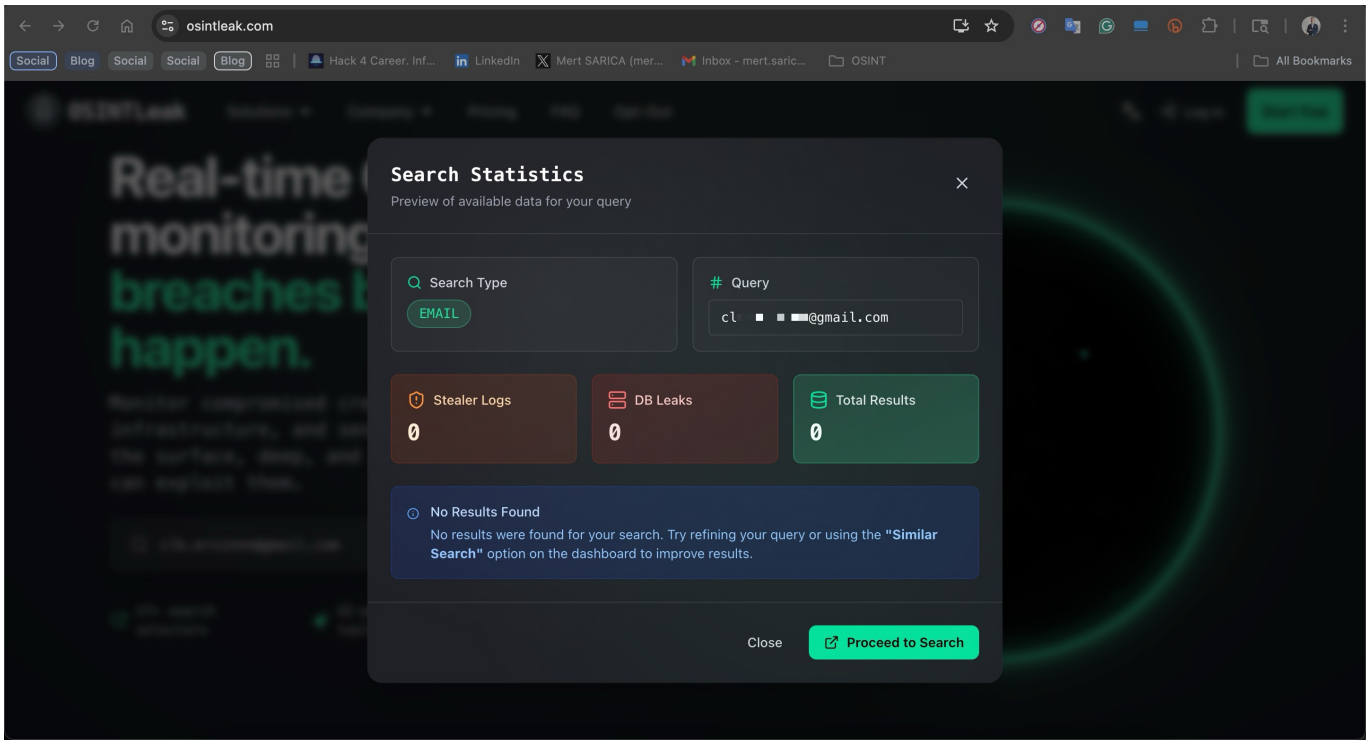


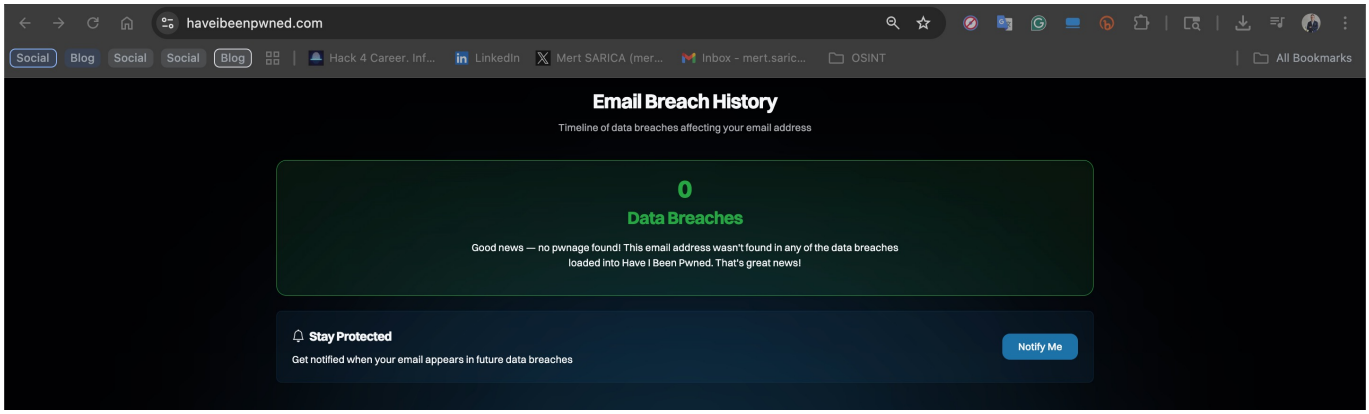
Bir diğer ekran görüntüsünde ise bu UUID / GUID değeri ile eşleştirilmiş bir kullanıcı bilgisini aradığımda, çok geçmeden bu kullanıcının adını, soyadını, e-posta adresini, TCKN'sini (245********) ve Istanbul Sende uygulamasına kayıt olduğu tarihi tespit ettim.

Öncelikle bu verilerin başka sızıntılardan, bilgi hırsızı zararlı yazılımlarından (infostealer) toplanıp, derlenen, sahte bir veri sızıntısı dosyası olmadığından emin olmak için ilk olarak ücretli SOCRadar platformunda örnek e-posta adresini arattım. Veri sızıntısına dair herhangi bir sonuçla

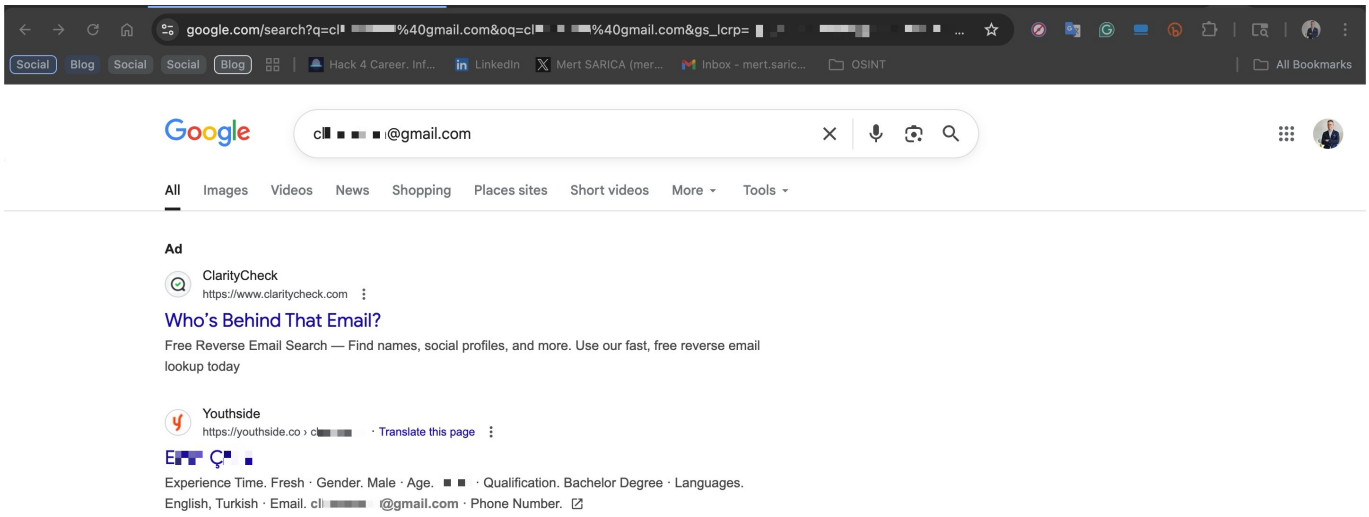
karşılaşmayınca ilave olarak bir de OSINTLeak, Have I Been Pwned gibi ücretsiz kaynaklarda arattım. Bunlarda da bir sonuçla karşılaşmayınca bu verilerin derleme, uydurma olmadığına kanaat getirdim.

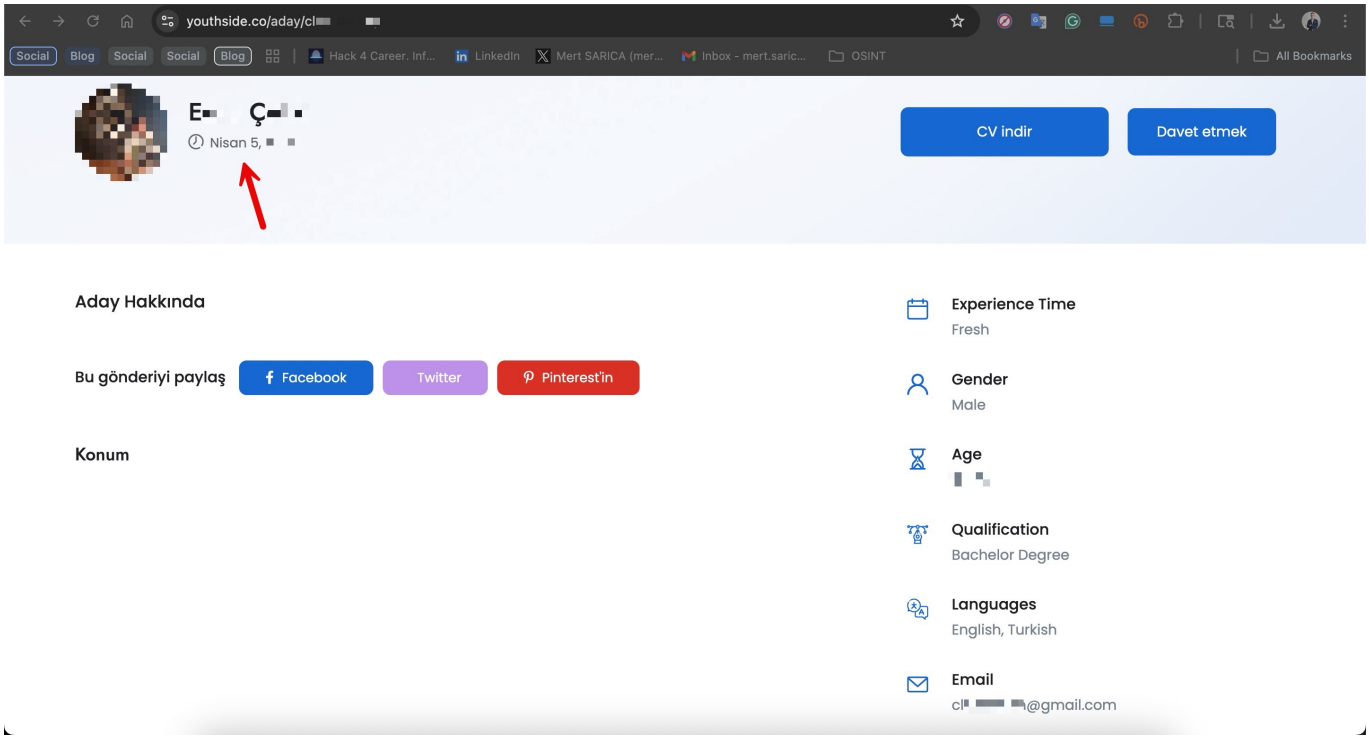


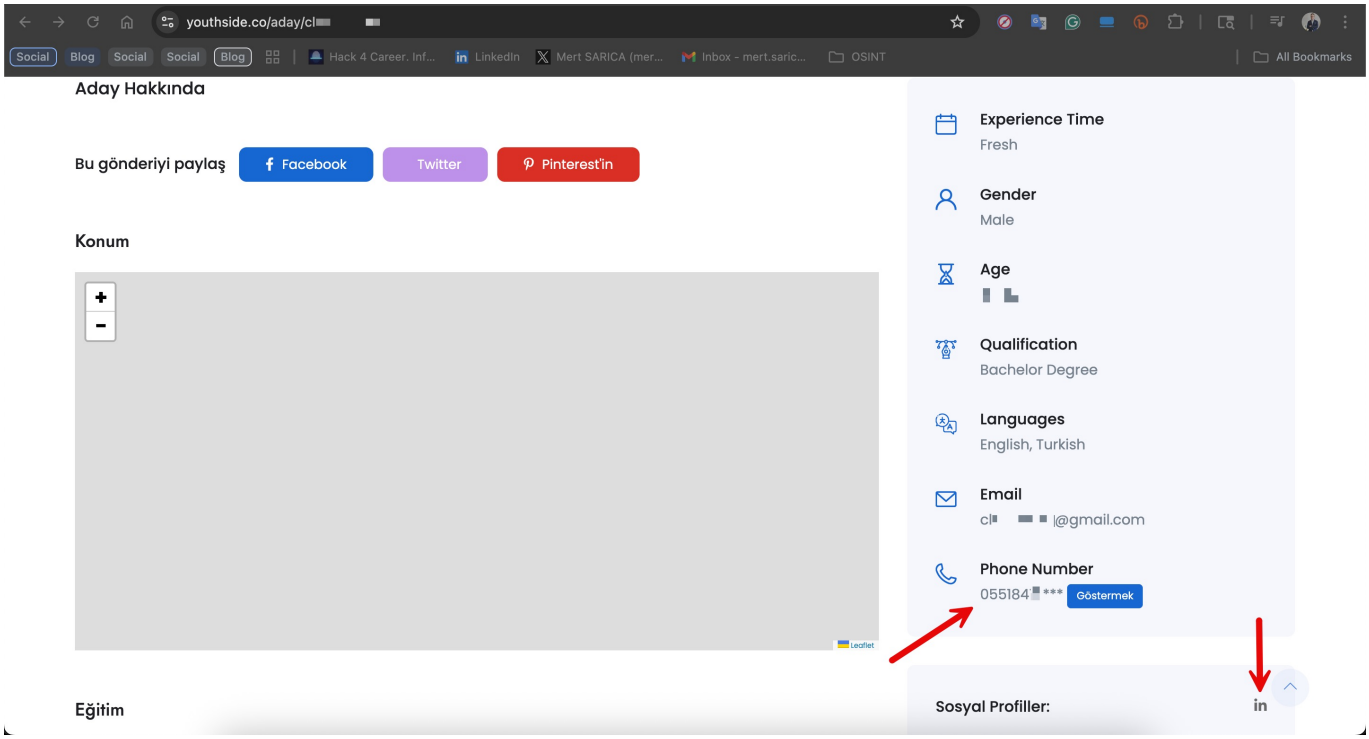




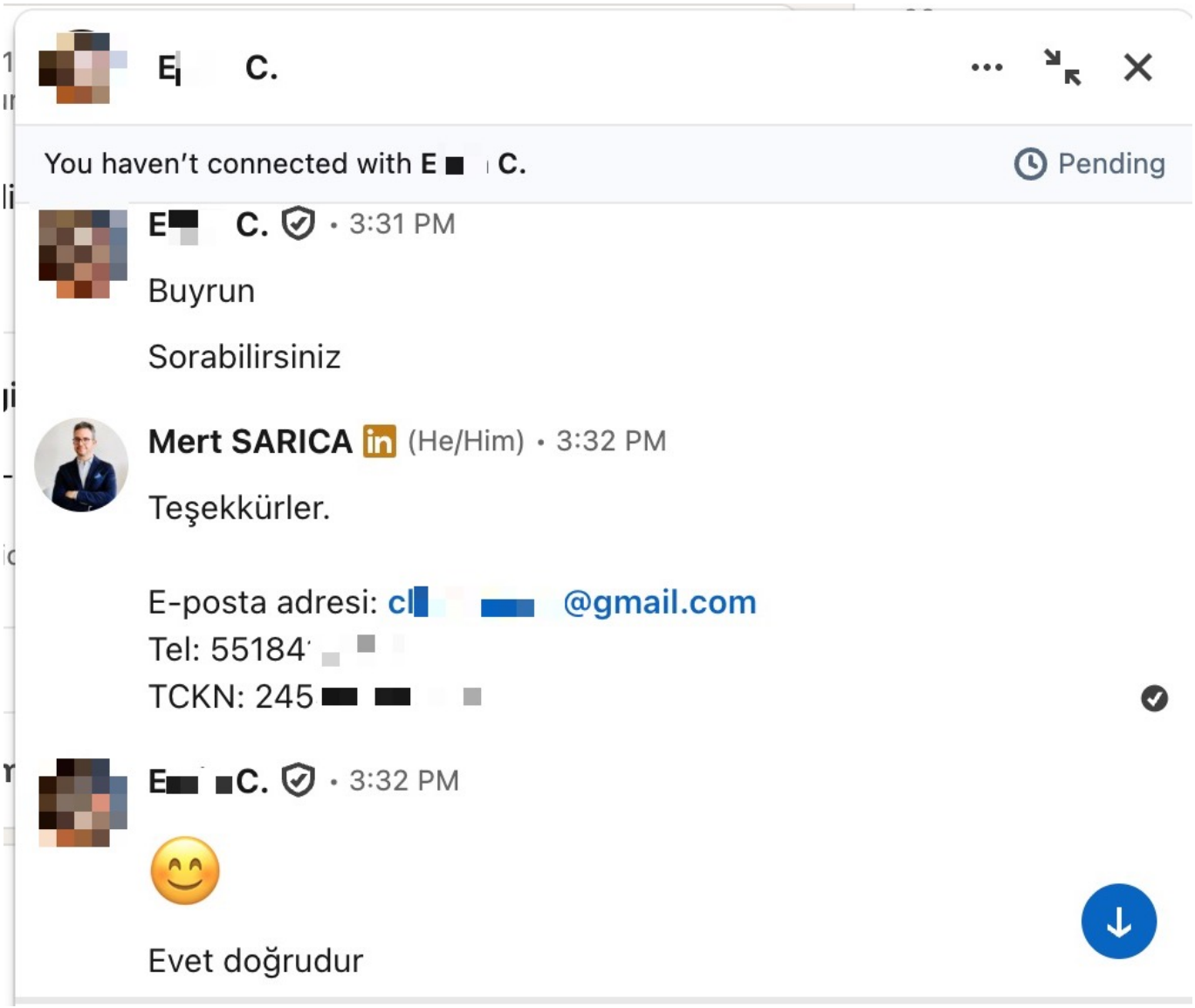
Sıra Açık kaynak istihbaratı (OSINT) ile genele açık araçlar üzerinden çalınan bu bilgileri doğrulamaya geldiğinde, Google arama motoru üzerinde yaptığım basit bir arama ile verisi çalınan vatandaşın Youthside isimli yeni nesil kariyer platformundaki genele açık bilgilerine ulaştım. Bu sayfa üzerinden ekran görüntülerinde geçen isim, soyad, e-posta adresi ve doğum tarihini doğrulayabildim.







Son olarak bu sayfada yer alan LinkedIn bağlantısı üzerinden bu kişi ile iletişime geçip, bilgileri doğrulamak için kendisine sormaya ve araştırmamı tamamlamaya karar verdim. Kendisi de sağolsun tüm sorularıma şeffaflıkla yanıt vererek bilgilerin doğruluğunu teyit etmiş ve bu sayede İstanbul Senin uygulamasına ait verilerin kuvvetme muhtemel art niyetli kişilerin eline bir şekilde geçmiş olduğunu anlamış oldum.



Sonuç

Sade bir vatandaş gözüyle işin teknik kısımlarına pek fazla girmeden, İBB'nin 'İstanbul Senin' uygulamasına yönelik soruşturmaya konu olan bilgilerin çalınıp çalınmadığını, 50.000$ ödemeden öğrenmiş ve red.eth gibi bunun nasıl yapılabileceğini merak edenlere bunu göstererek mutlu sona ulaşmış oldum. Bir veri kırıntısından yola çıkarak bir olayı nasıl doğrulayabildiğimi göstermeye çalıştığım bu yazı umuyorum ki zamanı geldiğinde ihtiyaç duyanlara yardımcı olur.

Bu yılın son yazısı olması vesileyle yeni yılınızı şimdiden kutlar, 2026 yılının hem sizlere hem de tüm sevdiklerinize önce sağlık sonra mutluluk ve başarı getirmesini dilerim.

Seneye görüşmek dileğiyle. :)