5 Şubat 2026

UZMAN MÜTALAASI

TUNCAY BEŞİKÇİ

Adli Bilişim Mühendisi (1. Sinif Onur Derecesi, Middlesex University, Birleşik Krallik)
Adli Bilirkişi (2013-2018, İstanbul Ceza Ve Hukuk Mahkemeleri No:7824)
Avrupa Birliği – Sertifikali Siber Adli Bilişim Profesyoneli (Ccfp-Eu No:440505)

Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

Sn. Av. ERKAM ERDEM,

5 Kasım 2025 tarihinde müvekkiliniz NECATİ ÖZKAN hakkında T.C. İSTANBUL CUMHURİYET BAŞSAVCILIĞI'nca yürütülen 2025/57354 numaralı soruşturma ile ilgili tamamı EK 1'de sunulan talep yazınızdaki sorularınıza ilişkin cevaplar, EK 2'de sunulan "Yasal Dayanak" başlıklı bölümünde belirtilen kanun maddeleri çerçevesinde, hiçbir baskı veya etki altında kalmadan, bilimsel olarak onaylı teknik düzenlemeler dikkate alınarak işbu Uzman Mütalaası tanzim edilerek 5070 sayılı elektronik imza kanununa göre güvenli elektronik imza ile imzalanarak sunulmuştur.

Uzman Kimliğime ilişkin bilgiler EK 3'de sunulmuştur. Raporda adı geçen kişi veya kurumlarla, bireysel veya kurumsal hiçbir ilişkim bulunmamaktadır.

Tuncay Beşikçi

Adli Bilişim Mühendisi (1. Sınıf Onur Derecesi, Middlesex University, Birleşik Krallık)
Adli Bilirkişi (2013-2018, İstanbul Ceza ve Hukuk Mahkemeleri No:7824)
Avrupa Birliği – Sertifikalı Siber Adli Bilişim Profesyoneli (CCFP-EU No:440505)

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

UYARI VE KISITLAMALAR

Bu rapor, somut olay kapsamında herhangi bir dijital cihaz, sistem veya hesap üzerinde adli imaj alma, canlı analiz ya da veri çıkarımı yapılmaksızın hazırlanmıştır. İnceleme; açık kaynak istihbaratı (OSINT) yöntemleri, Darkweb pazarları, forumlar ve servisler ile açık internet üzerindeki teknik ve operasyonel verilerin derlenmesi, karşılaştırılması ve analitik değerlendirilmesi ile sınırlıdır. Bu nedenle rapor, doğrudan fail tespiti veya kişiye atfedilebilir teknik kesinlik iddiası içermez.

Darkweb ve internet ortamlarında yer alan içerikler; anonimlik, geçicilik, manipülasyona açıklık ve kaynak güvenilirliğinin değişkenliği gibi özellikler taşır. Bu raporda kullanılan bulgular, çoklu kaynak doğrulaması, zaman damgası tutarlılığı ve içerik-kaynak çapraz kontrolü esaslarıyla değerlendirilmiş olsa da, üçüncü taraf içeriklerinin mutlak doğruluğu garanti edilemez.

İncelemeye konu platformlar ve içerikler dinamik olup, raporun hazırlandığı tarihten sonra erişilemez hale gelmiş, değiştirilmiş veya silinmiş olabilir. Bu durum, rapor bulgularının rapor tarihi itibarıyla geçerli olduğu anlamına gelir; sonradan ortaya çıkan değişiklikler rapor kapsamı dışındadır.

Raporda yer alan değerlendirmeler; teknik, operasyonel ve istihbari göstergelerin bir arada yorumlanmasına dayanır. IP adresi, kullanıcı adı, takma ad (nickname), kripto adresi, forum profili veya ilan gibi göstergeler tek başına kişiye kesin atıf için yeterli değildir. Bu göstergeler olasılık ve senaryo düzeyinde ele alınmış, kesin kimliklendirme yapılmamıştır.

Bu rapor, hukuki vasıflandırma veya suçun unsurlarının oluşup oluşmadığına dair nihai değerlendirme yapmaz. Rapor; teknik bulguların adli bilişim perspektifinden açıklanması ile sınırlıdır. Kişisel verilerin hukuka aykırı elde edilmesi/sızdırılması ve casusluk gibi suç tiplerine ilişkin hukuki takdir, münhasıran mahkemenin yetkisindedir.

İnceleme sırasında, gereksiz kişisel veri ifşasından kaçınılmış, yalnızca iddiaların teknik olarak anlaşılmasına hizmet eden veriler rapora dahil edilmiştir. Rapor, özel hayatın gizliliği ve veri minimizasyonu ilkeleri gözetilerek hazırlanmıştır.

Kullanılan yöntemler; erişilebilirlik, tekrarlanabilirlik ve orantılılık ilkelerine uygun seçilmiştir. Ancak, platformların kendi iç kayıtları, servis sağlayıcı logları veya yetkili makamlarca temin edilebilecek kapalı kaynak veriler bu rapor kapsamında değildir. Bu tür verilerle yapılacak ek incelemeler, sonuçları değiştirebilir veya güçlendirebilir.

Darkweb ve internet ekosisteminin doğası gereği, raporda sunulan teknik açıklamalar alternatif senaryoları dışlamaz. Bulgular; en makul teknik açıklamalar çerçevesinde değerlendirilmiş olup, tekil ve mutlak senaryo iddiası taşımamaktadır.

Bu rapor, avukat sorularına teknik açıklama sağlamak, iddiaların teknik çerçevesini ortaya koymak ve mahkemenin değerlendirmesine yardımcı olmak amacıyla hazırlanmıştır. Raporun, bağlamı dışında veya seçici alıntılarla kullanılması, teknik anlamı bozabilir.

TUNCAY BEŞİKÇİ

Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

KAPSAM

Uzman Mütalaasının kapsamı, ERDEM AVUKATLIK BÜROSU'ndan Av. Erkam Erdem'in 5 Kasım 2025 tarihli talep yazısındaki (EK1) soruların, uzmanlık alanlarım çerçevesinde incelenerek cevaplandırılmasından ibarettir.

Uzman Mütalaası içeriğinde, CMK[1], Yargıtay içtihatları ve bilirkişilik mevzuatı[2] ve uluslararası Adli Bilişim standartlarına[3] bağlı kalınmaya özen gösterilmiş, Uzman Mütalaası kapsamında teknik referans ve kaynaklar dipnotlarda belirtilmiştir.

İnceleme, tarafıma dijital ortamda gönderilmiş ve aşağıda listesi sunulan dijital dokümanlar üzerinde gerçekleştirilmiştir.

- 26 Ekim 2025 tarihli, Şüpheli HÜSEYİN GÜN'e ait ifadelerin yer aldığı anlaşılan Şüpheli İfade Tutanağı
- 26 Ekim 2025 tarihli, T.C. İSTANBUL CUMHURİYET BAŞSAVCILIĞI'nca Şüpheli HÜSEYİN GÜN için düzenlenmiş Sorgulama Tutanağı
- 26 Ekim 2025 tarihli, T.C. İSTANBUL 12. SULH CEZA HAKİMLİĞİ'nce Şüpheli NECATİ ÖZKAN için düzenlenmiş 2025/944 numaralı Sorgu Tutanağı
- 12 Aralık 2025 tarihli, T.C. İSTANBUL 40. AĞIR CEZA MAHKEMESİ'nce 2025/318 E numaralı dosya için düzenlenmiş Tensip Zaptı

Soruşturmanın seyrine göre, ilave dijital kanıtlar ve uzman raporları ortaya çıkabileceğinden, burada yapılan analiz yeni bulgularla güncellenebilir. İşbu Uzman Mütalaası yalnızca tarafıma sunulan mevcut bilgiler ve açık kaynak veriler ışığında hazırlanmıştır.

[1] Ceza Muhakemesi Kanunu
[2] 6754 sayılı Bilirkişilik Kanunu
[3] ISO/IEC 27037, ISO/IEC 27042, ISO/IEC 27043, ISO/IEC 17025, Scientific Working Group on Digital Evidence, National Institute of Standards and Technology

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734896, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

TESPİT VE BULGULAR

Yapılan incelemeler sonucunda talep yazısında yöneltilen sorular başlıklar halinde cevaplandırılmış, bazı teknik açıklamalar dipnotlarda ve Uzman Mütalaası eklerinde sunulmuştur.

1. Soruşturma kapsamında geçen OSINT ve Darkweb kavramları nedir?

OSINT (Open Source Intelligence - Açık Kaynak İstihbaratı), hukuka uygun şekilde herkesin erişimine açık bilgi kaynaklarından elde edilen verilerin toplanması, doğrulanması ve analiz edilmesi sürecidir[4].

OSINT kapsamında; İnternet siteleri, açık forumlar, sosyal medya platformları, açık veri tabanları, akademik ve teknik yayınlar incelenir.

Bu yöntemde yetkisiz erişim, gizli veri elde etme veya sistemlere sızma söz konusu değildir [1].

Adli bilişim literatüründe OSINT, doğrudan suç isnadı veya fail tespiti için değil, teknik iddiaların bağlamsal olarak değerlendirilmesi, iddiaların makuliyetinin test edilmesi ve senaryo analizi amacıyla kullanılan destekleyici bir yöntem olarak kabul edilmektedir[5][6].

Bu raporda OSINT, kişisel verilerin sızdırıldığı iddiasının teknik olarak mümkün olup olmadığının değerlendirilmesi ve çevrim içi ortamlardaki genel yöntemlerin anlaşılması amacıyla kullanılmıştır.

Darkweb, standart internet tarayıcılarıyla erişilemeyen ve özel yazılımlar (örneğin Tor[7] ağı) aracılığıyla ulaşılan ağ yapılarının genel adıdır[8].

Darkweb'in kullanımı tek başına hukuka aykırı değildir. Bu ağlar;

- İfade özgürlüğü,
- Sansürden kaçınma,
- Gizlilik ihtiyacı gibi meşru amaçlarla da kullanılabilmektedir [6].

Ancak anonimlik sağlaması nedeniyle Darkweb ortamlarında, hukuka aykırı yollarla elde edildiği iddia edilen kişisel verilerin paylaşımı gibi faaliyetlere de rastlanabilmektedir. Akademik çalışmalar, Darkweb üzerindeki paylaşımların çoğu zaman doğrulanmamış, yanıltıcı veya manipülatif olabileceğini ortaya koymaktadır[9].

Bu nedenle Darkweb üzerinde görülen bir içerik;

- Paylaşımı yapan kişinin kimliğini kesin olarak göstermez,
- Verinin gerçekliğini tek başına ispatlamaz,
- Hukuki sorumluluğu otomatik olarak belirlemez.

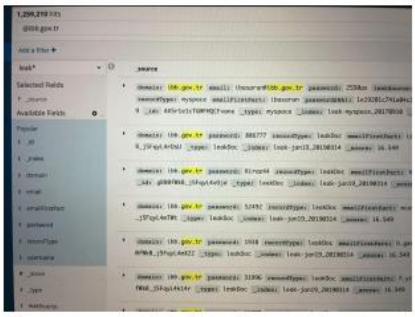
---

[4] *NIST SP 800-86 – Guide to Integrating Forensic Techniques into Incident Response*.
[5] ISO/IEC 27043:2015, *Incident investigation principles and processes*.
[6] (SWGDE), *Best Practices for Digital Evidence*
[7] https://support.torproject.org/tr/about-tor/introduction/what-is-tor/
[8] (ENISA), *Exploring the Darknet*, 2018. (https://www.enisa.europa.eu/)
[9] Holt, T. J., *Dark Web Markets and Cybercrime*, Journal of Cybercrime Studies.

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

2. *Soruşturma kapsamındaki şüphelilerden Hüseyin Gün'ün açık kaynaklarda yer alan Emniyet ifadesinin, 124 ve 125. sayfalarında geçen ve İstanbul Büyükşehir Belediyesi'ne ait olduğu iddia edilen veriler nelerdir?*





124 ve 125. sayfalarda bulunan İBB verileri, bir bilgisayar monitöründen fotoğraflandığı anlaşılan, web tabanlı bir arama uygulamasının sonuç ekranında görüntülenen ibb.gov.tr uzantılı e-mail adresleridir.

Ekran görüntülerdeki bilgiler; isfalt@ibb.gov.tr, h.karakaya@ibb.gov.tr, mcavus@ibb.gov.tr, h.gencal@ibb.gov.tr, f.yilmaz@ibb.gov.tr, h.zeyveli@ibb.gov.tr, nefise.uygun@ibb.gov.tr, naile.sen@ibb.gov.tr, saliha.peru@ibb.gov.tr, hsan@ibb.gov.tr, beyazmasa@ibb.gov.tr, alpergo@ibb.gov.tr, burhanayan@ibb.gov.tr, adilyildirim@ibb.gov.tr, i.basaran@ibb.gov.tr. bozkul@ibb.gov.tr ve ikizzeynep.mutlu@ibb.gov.tr e-mail adreslerin oluşmuştur.

Bu İBB e-posta adreslerinin, büyük veri üzerinde arama yapmak için geliştirilmiş web tabanlı bir uygulamada görüntülendiği anlaşılmaktadır. İnternet üzerinde çok sayıda benzer uygulama bulunmaktadır. Örneğin *OSINTLeak* adlı ticari platform, e-posta adresleri, kullanıcı adları, telefon numaraları gibi çok sayıda farklı alanda arama yapabilen, gerçek zamanlı sızıntı takibi sunan bir çözüm sunmaktadır[10].Benzer şekilde, siber güvenlik uzmanları da kendi ihtiyaçlarına yönelik özel arama sistemleri geliştirmektedir. Örneğin, 2025 yılında genç bir Türk tarafından tanıtılan "Elastic Leak Searcher" adlı araç, Elasticsearch [11] arama altyapısını kullanarak karanlık ağdan elde edilen kimlik bilgisi sızıntılarını hızlıca tarayıp analiz etmeyi hedefleyen bir projedir[12]. Bu tür örnekler, kurumsal güvenlik ekiplerinin veya adli bilişim uzmanlarının büyük hacimli sızdırılmış verileri aramak için genellikle NoSQL[13] tabanlı, dağıtık ve ölçeklenebilir arama motorlarına başvurduğunu göstermektedir[14]. Fotoğraflarda görünen arayüz de bu kapsamda, Elasticsearch gibi bir büyük veri arama altyapısı üzerinde çalışan, özel geliştirilmiş bir uygulamadır.

Ekran görüntüsünde listelenen veritabanı alanları, NoSQL tabanlı bir veri tabanının tipik indeks kayıtlarını yansıtmaktadır. Bu alanların işlevleri ve NoSQL karşılıkları şu şekilde açıklanabilir:

_id: Her bir kaydın benzersiz kimliğini temsil eden alan

[10] https://osintleak.com/
[11] https://www.elastic.co/elasticsearch
[12] https://www.linkedin.com/posts/onurcangnc_credential-leak-intelligence-elastic-leak-activity-7336538889135841280-AG_Q/
[13] "NoSQL" terimi, ilişkisel olmayan veritabanı türlerini ifade eder ve bu veritabanları verileri ilişkisel tablolardan farklı bir formatta depolar.

[14] https://hackread.com/elasticsearch-leak-6-billion-record-scraping-breaches/

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

_type: Bu alan, ilgili dokümanın türünü veya kategorisini belirtir.

domain (alan adı): Sızdırılan e-posta adresinin @ işaretinden sonraki kısmını, yani ait olduğu domain'i ifade etmektedir.

emailFirstPart: Bu alan, e-posta adresinin @ işaretinden önceki kısmını, yani kullanıcı adı kısmını içerir.

password (şifre): Bu alan, ilgili e-posta adresi veya hesabın sızdırılmış parolasını içerir.

t_score: Bu alan arama motorunun ilgili kayda verdiği skor değeridir. Sıralama amaçlı kullanılır.

Yukarıdaki alanların tümü, NoSQL ve arama motoru teknolojilerinde büyük veri setlerini yönetmek ve hızlı sorgulamak için tasarlanmış yapılara uygundur. Örneğin Snusbase[15] gibi 10 milyarlarca kayıt içeren sızıntı arama motorlarında her bir kayıt; _id (benzersiz kimlik), email (tam e-posta), _domain (alan adı), password gibi alanlarla depolanmakta ve indekslenmektedir. Bu sayede tek bir e-posta adresinin veya alan adının var olup olmadığını sorgulamak çok büyük verilerde bile mümkün hale gelir.

Ekran görüntüsünde, arama kutucuğuna *"leak"** şeklinde bir ifade girildiği görülmektedir. Yıldız (*) karakterinin kullanılması, bu sistemin büyük ihtimalle Elasticsearch benzeri bir full-text arama altyapısı kullandığına işaret eder. Elasticsearch'te ve benzeri arama dillerinde * joker karakteri, herhangi bir metin ile eşleşebilen joker karakter olarak kullanılır[16].

Sorguda, Türkçede "sızıntı" anlamına gelen **leak*** yazılması, "leak" ile başlayan tüm kategorilerdeki sonuçları aramak hedeflenmiştir. Nitekim, arama sonuçlarında "leakDoc" ve "leak-myspace_20170910" kategorilerindeki sonuçlar filtrelenmiştir. Arayüzdeki filtreleme yetenekleri değerlendirildiğinde, kullanıcıların veritabanında belirli bir sızıntı kümesini, tarih aralığını veya alan adını filtreleyebildiği anlaşılmaktadır.

İlgili arayüzün temel amacı, sızdırılmış e-posta, kullanıcı hesabı ve parola verilerini aratıp bulmak ve detaylarıyla sunmaktır. Ekran görüntüsünden anlaşıldığı kadarıyla, arama sonuçlarında her bir kayıt JSON benzeri bir yapıda listelenmekte ve içinde söz konusu hesap bilgilerinin yanı sıra kaynağa dair üstveri (metadata) alanları da bulunmaktadır. Bu bağlamda **recordType, _index** ve **leakSource** alanları sızıntıların kaynakları ve tarihleri hakkında bilgi verdikleri anlaşılmaktadır.

Her iki sayfadaki üstveri bilgilerinden sızan İBB verilerinin **leak-myspace_20170910** ve **leak-jan19_20190314** isimleri altında bulunduğu anlaşılmaktadır. Bu isimler **10 Eylül 2017** tarihli **MySpace** ve **14 Mart 2019** tarihinde yüklenen **19 Ocak** sızıntılara işaret etmektedir.

Yapılan incelemelerde, arayüzde sızıntı kaynakları için kullanılan isimlerin geçmişte gerçekleşen veri sızıntıları ile tutarlı olduğu anlaşılmıştır.

Sosyal paylaşım sitesi MySpace şirketinin 31 Mayıs 2016 tarihinde resmi İnternet sayfasından yaptığı açıklamada[17], Anma Günü hafta sonundan kısa süre önce, çalınmış Myspace kullanıcı giriş bilgilerinin çevrim içi bir hacker forumunda paylaşıldığının tespit edildiği, çalınan verilerin eski Myspace platformunda 11 Haziran 2013'ten önce oluşturulmuş hesapların bir kısmına ait kullanıcı giriş bilgilerini kapsadığı, bu saldırının **Rus siber korsan "Peace"** adlı kişinin olduğu, aynı kişinin LinkedIn ve Tumblr şirketlerine yapılan saldırılardan da sorumlu olduğu ve

[15] Snusbase
[16] https://discuss.elastic.co/t/searching-emails-by-domain/69550
[17] https://myspace.com/pages/blog

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

ücretli hacker arama motoru **LeakedSource**[18] üzerinden verilerin geçmişteki bir ihlale ait olduğunu iddia ettiğini açıklamıştır.


BBC NEWS TÜRKÇE

Haberler Türkiye Ortadoğu Rusya-Ukrayna Savaşı Ekonomi Sağlık Bilim Teknoloji

360 milyon MySpace ve Tumblr hesabı çalındı

Manşet haber

Doğum izninin uzatılması kadınların iş hayatına katılımını nasıl etkileyecek?

9 saat önce

31 Mayıs 2016

Sosyal paylaşım siteleri MySpace ve Tumblr'dan çalınan yüzlerce milyon hesap bilgileri internette satışa çıkarıldı. Bilgilerin birkaç yıl önce çalındığı, ancak durumun yeni anlaşıldığı ortaya çıktı.


euronews.

Son haberler Avrupa Dünya Business Gezi Next Kültür Green Sağlık Video

Haber > Dünya > ABD

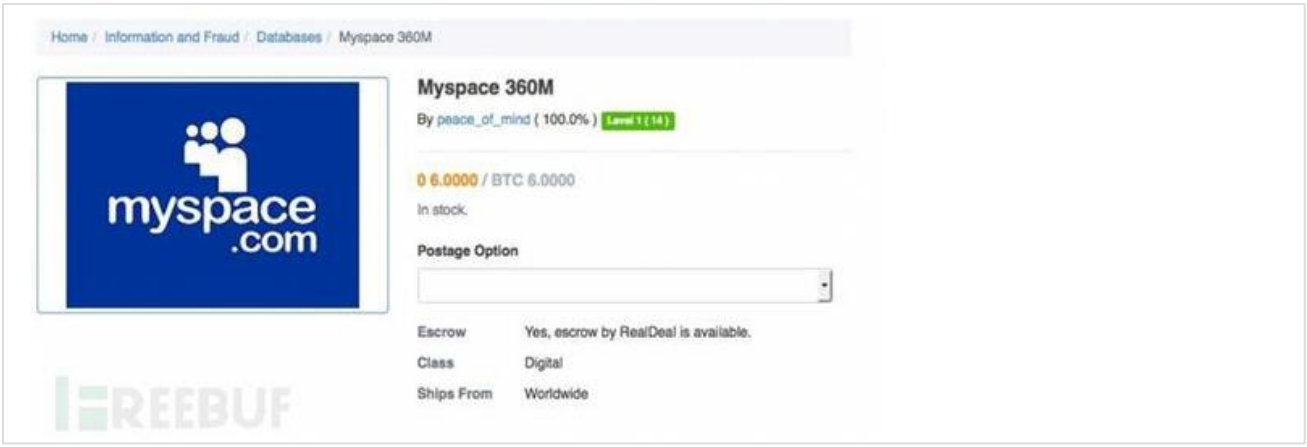
MySpace ağına ait milyonlarca hesap bilgisi çalındı

By Euronews

Yayınlanma Tarihi 01/06/2016 - 23:21 GMT+2

Sosyal paylaşım ağlarının ilklerinden MySpace platformunun siber saldırıya uğradığı ve milyonlarca hesabın çalındığı ortaya çıktı.

Sonuç olarak, aralarında **MySpace** sitesine **i.basaran@ibb.gov.tr** kullanıcı adı ve **2550as** şifresi ile kaydolan bir şahsın da bulunduğu **359.1 milyon** hesabın[19] **Temmuz 2008**'de "**Peace**" takma adını kullandığı bildirilen tehdit aktörü tarafından ele geçirildiği, bu bilgilerin **31 Mayıs 2016** tarihinde Darkweb'de bulunan "**The Real Deal**" isimli sitede **6 Bitcoin** *(yaklaşık 2800-3000 dolar)* ücretle **satıldığı**[20] anlaşılmış, söz konusu satış ilanına ait ekran görüntüsü aşağıda sunulmuştur.



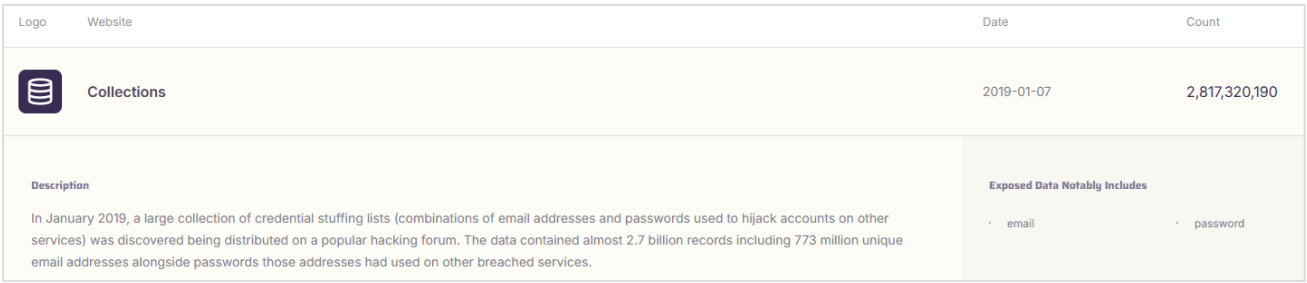
Yapılan incelemelerde, ekran görüntülerinde yer alan diğer tüm İBB e-posta adreslerin de benzer şekilde **Ocak 2019** sıralarında "**Collections**" (Koleksiyonlar) ismiyle Darkweb'e sızdırıldığı anlaşılmıştır. Aralarında **12,000**'den fazla web sitesinin bulunduğu[21] **2,890** ayrı kaynaktan ele geçirilerek derlendiği tespit edilen **772,904,991** kullanıcı adı ve **21,222,975** şifrenin yer aldığı **87GB** büyüklüğündeki veritabanı içeriğinde ibb.gov.tr veya İBB'ye ait herhangi bir şirkete rastlanmamıştır[22]. Sonuç olarak, inceleme konusu fotoğraflardaki verinin, üyelik vb. nedenlerle İBB e-posta adreslerinin kullanıldığı farklı web sitelerinden ele geçirildiği anlaşılmıştır.

Sızdırılmış veri ihlallerinden elde edilen e-posta adresleri, kullanıcı adları, parolalar, IP adresleri ve alan adlarının indekslenerek OSINT ve siber güvenlik araştırmalarında yetkili kullanıcıların bu veriler üzerinde arama ve doğrulama yapmasına imkân tanıyan, ticari ihlal veri analizi

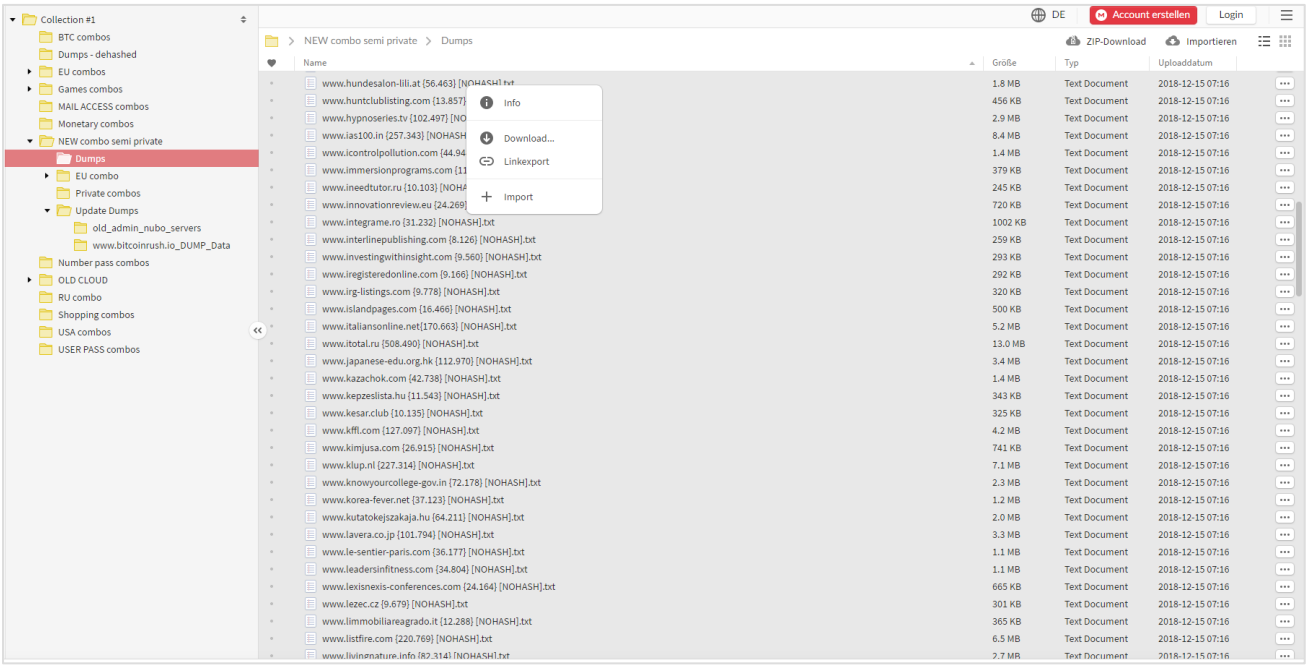
[18] https://www.leakedsource.com/
[19] https://haveibeenpwned.com/breach/MySpace
[20] https://www.wosign.com/English/News/myspace.html
[21] https://www.edoardolimone.com/file/cybersec/collections/posta_difesa_esercito.txt
[22] Veri ihlali saldırısına uğrayan 2,890 kaynağın listesi: https://h7.cl/1gqHU

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

platformu DeHashed [23] verilerine göre Collections adlı sızıntının **7 Ocak 2019** tarihinde gerçekleştiği anlaşılmış, ilgili ekran görüntüsü aşağıda sunulmuştur.



7 Ocak 2019 tarihli sızıntının ilk olarak MEGA[24] isimli dosya paylaşım platformuna yüklendiği anlaşılmış[25] dosyaların paylaşıldığı ekran görüntüsü aşağıda sunulmuştur.



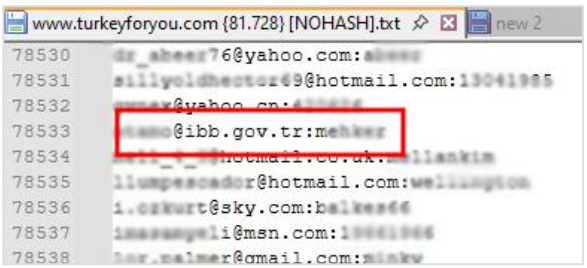
"Collections" isimli veri setindeki dosyaları içeren yukarıdaki sayfanın linkleri yalnızca Darkweb de değil İnternet üzerinde çok sayıda forum ve sosyal medyada paylaşıldığı anlaşılmıştır. Veri setinde veri ihlaline uğramış Türkçe içerikli bazı siteler, veri ihlaline uğradığı tarih ve sızan kullanıcı sayısı bilgileri aşağıdaki tabloda sunulmuştur.

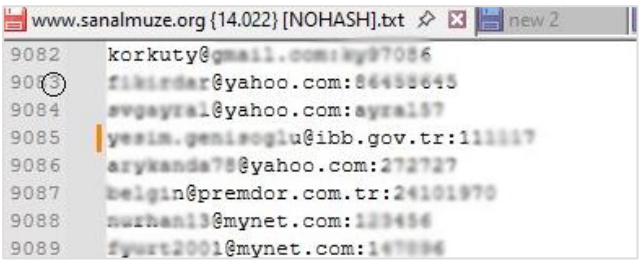
Alan Adı	Açıklama	Veri İhlal Tarihi	Kullanıcı
akademikbakis.org	Uluslararası hakemli sosyal bilimler dergisi	3 Haziran 2018	2.019
atak-tekstil.com	Türkiye merkezli şirket	13 Mayıs 2018	6.179
gelecekdaha.net	Gençlik platformu	11 Haziran 2018	2.747
hermeskitap.com	Online kitap satış mağazası	3 Aralık 2017	27.493
egitimsenistanbul7.org	Eğitim-Sen, İstanbul şubesi	24 Kasım 2017	16.428

[23] https://dehashed.com/
[24] https://mega.io/
[25] https://gizmodo.com/mother-of-all-breaches-exposes-773-million-emails-21-m-1831833456

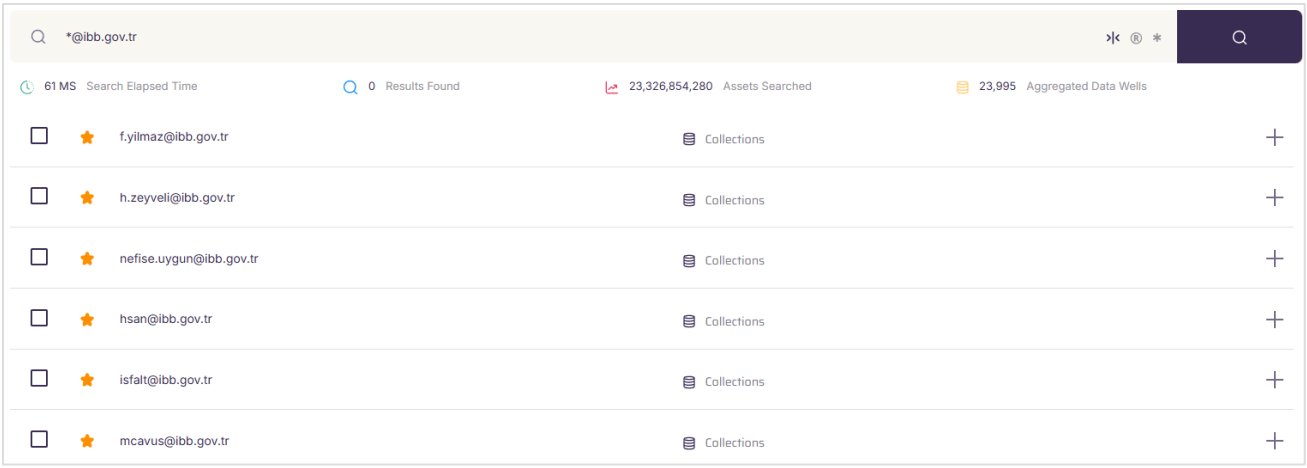
TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

Örneğin inceleme konusu olayda, **turkeyforyou.com** adresli turizm amaçlı siteye İBB e-postası ile üye olan bir İBB çalışanının e-mail adresi ve bu site için oluşturduğu şifre, **2017** yılında diğer **81,728** site üyesiyle, aynı şekilde, Eczacıbaşı Holding tarafından 1999 yılında açılan **sanalmuze.org** isimli siteye üye olan bir başka İBB çalışanına ait giriş bilgileri **2016** yılında diğer **14,022** Sanal Müze üyesiyle birlikte siber korsanların eline geçmiştir.





Hüseyin Gün'e ait ifadede yer alan İBB e-posta adresleri dehashed.com sitesinde aratıldığında 7 Ocak 2019 tarihinde sızan "Collections" veri seti içinde oldukları anlaşılmış, ilgili ekran görüntüsü aşağıda sunulmuştur.

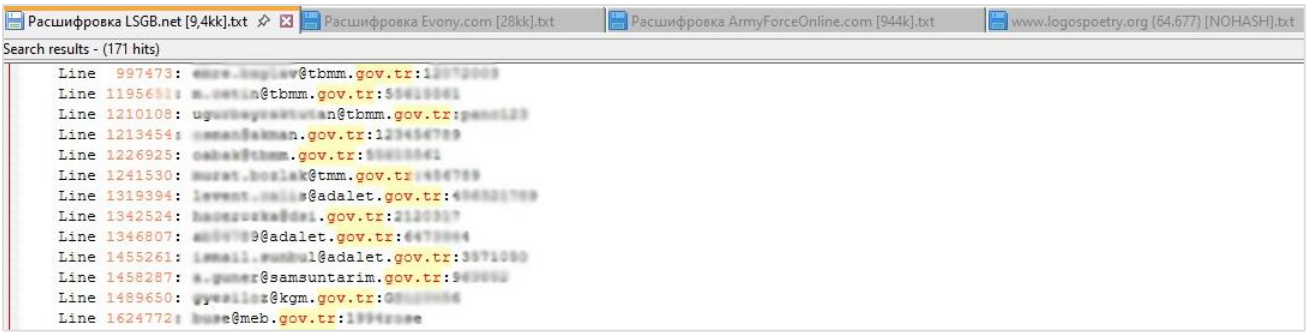


7 Ocak 2019 tarihinde 12 binden fazla İnternet sitesi arasından rastgele seçilen **5** tanesinde[26] **"gov.tr"** anahtar kelimesi ile yapılan arama sonuçlarında, İBB haricinde aralarında TBMM, Adalet Bakanlığı, EGM, MEB, TÜBİTAK gibi kritik kurumların da bulunduğu **57** devlet kurumundan[27] **171** kamu görevlisinin gov.tr uzantılı e-mail adresleri ile birlikte bu sitelerde kullandıkları şifrelerin siber korsanlarca ele geçirildiği anlaşılmış, sonuçların bir kısmına ait ekran görüntüsü aşağıda sunulmuştur.

[26] Rastgele seçilen siteler: Yazılım indirme sitesi LSGB.net, şiir sitesi logospoetry.org, oyun sitesi evony.com,

[27] Rastgele seçilen sitelerde bulunan devlet kurumlarına ait alan adları: adalet.gov.tr, aile.gov.tr, akman.gov.tr, buski.gov.tr, byegm.gov.tr, csb.gov.tr, denizli-bld.gov.tr, dhmi.gov.tr, die.gov.tr, dmo.gov.tr, dsi.gov.tr, egm.gov.tr, etimaden.gov.tr, eximbank.gov.tr, gap.gov.tr, gov.tr, hazine.gov.tr, ibb.gov.tr, igeme.gov.tr, ilbank.gov.tr, imkb.gov.tr, iskur.gov.tr, kgm.gov.tr, kik.gov.tr, kosgeb.gov.tr, mam.gov.tr, meb.gov.tr, mfa.gov.tr, milliemlak.gov.tr, mrb.gov.tr, mta.gov.tr, muhasebat.gov.tr, nukleer.gov.tr, oib.gov.tr, osmangazi-bld.gov.tr, osym.gov.tr, ptt.gov.tr, saglik.gov.tr, samsuntarim.gov.tr, sanayi.gov.tr, sgb.gov.tr, spk.gov.tr, ssm.gov.tr, taek.gov.tr, tagem.gov.tr, tbmm.gov.tr, tcmb.gov.tr, telekom.gov.tr, tetas.gov.tr, tkgm.gov.tr, tmm.gov.tr, tmo.gov.tr, todaie.gov.tr, tubitak.gov.tr, ulakbim.gov.tr, ume.tubitak.gov.tr, ubak.gov.tr

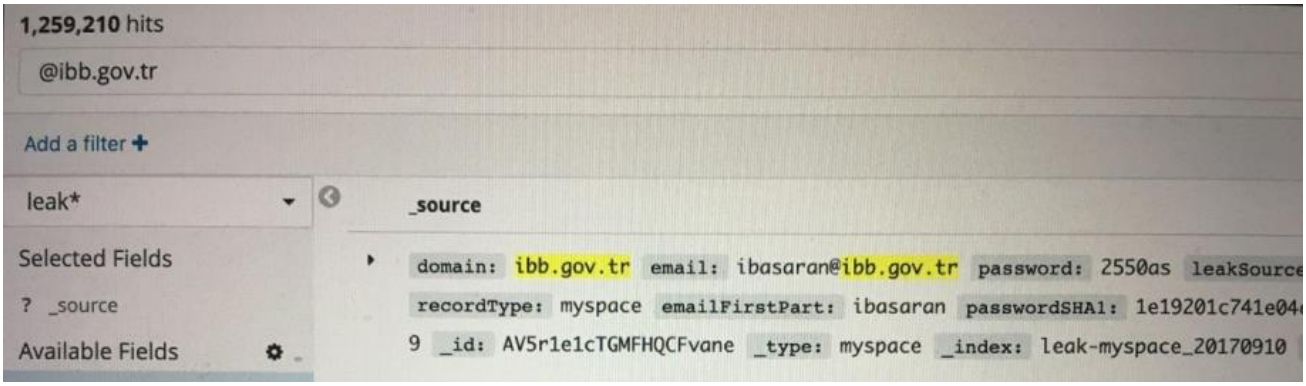
TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0



Yapılan araştırmalarda, inceleme konusu sızıntının "**Sanix**" olarak bilinen siber korsan tarafından derlendiği fakat rakibi "**Azatej**" olarak bilinen siber korsan tarafından sızdırıldığı tespit edilmiştir. Her iki siber korsan Avrupa Polis Teşkilatı Europol tarafından tespit edildikten sonra[28] **Polonya** ve **Ukrayna'da** yakalanıp[29] hapse atıldıkları anlaşılmıştır[30].

3. Darkweb'ten alındığı belirtilen bu veriler yine 125. sayfada yer alan ekran görüntüsü uyarınca, hangi anahtar kelime ya da kelimeler aratılarak bulunmuş, spesifik bir isim ya da bilgi girilmiş midir?

125. sayfadaki ekran görüntüsüne göre arama **"@ibb.gov.tr**" anahtar kelimesi ile yapılmış, herhangi spesifik bir isim ya da bilgi belirtilmemiş, Türkçede "sızıntı" anlamına gelen **leak*** yazılarak "leak" ile başlayan tüm veri setleri hedeflenmiş ve arama sonucunda eşleşen **1,259,210** kayıt bulunmuştur.



Söz konusu ekran görüntüsünden spesifik olarak özel bir şahıs ismi girilmediği ve yalnızca sızan bilgiler arasında içeriğinde "@ibb.gov.tr" geçen verinin aratıldığı anlaşılmaktadır.

4. Yine bu kapsamda İBB'den alınan ve ekte sunulan cevabi yazı uyarınca, suçlama konusu yapılan İBB personellerinin e-posta adres ve şifreleri dikkate alınarak, bu kişilerden bazılarının 2019 yılından önce İBB'den ayrıldıkları değerlendirildiğinde, bu kişilerin e-posta ve şifrelerinin 2019 yılı itibarıyla Darkweb'te yer almasının bir

[28] https://www.zdnet.com/article/europol-arrests-hackers-behind-infinity-black-hacker-group/

[29] https://web.archive.org/web/20200521012054/https://ssu.gov.ua/ua/news/1/category/2/view/7602#.jnAqqCRr.dpbs

[30] https://www.europol.europa.eu/media-press/newsroom/news/hacker-group-selling-databases-millions-of-user-credentials-busted-in-poland-and-switzerland

önemi bulunmakta mıdır, bu kişilerin e-posta ve şifreleri hangi yılda Darkweb'e yüklenmiş olabilir?

İnceleme konusu sızan verilerin farklı sitelerde üyelikler için kullanılmış oldukları, İBB sistemlerinden ele geçirilmedikleri, dolayısıyla söz konusu şifrelerin İBB sistemlerine giriş için kullanılamayacağı, şifreler doğru olsa dahi İBB'nin kullandığı Microsoft Outlook e-posta sisteminin[31] yeni cihaz girişlerinde ekstra güvenlik protokolü uygulayacağı ve inceleme konusu e-maillere ait basit şifrelerle[32] sisteme erişim izni vermeyeceği için siber güvenlik açısından yüksek seviyede ciddi bir risk oluşturması beklenmemektedir.

Yapılan incelemelerde, **7 Ocak 2019** tarihinde sızan veri içeriğindeki ilk ele geçirilen sitenin tarihi **29 Ağustos 2008** olarak tespit edilmiştir[33]. **31 Mayıs 2016**'da sızan verinin ise **Temmuz 2008**'de ele geçirildiği açıklanmıştır. Diğer bir ifadeyle, siber korsanların 8-10 yıl süreyle aktif olarak topladıkları verilerin **2019** tarihinden çok önce ele geçirilip kullanılmaya başlanmıştır.

2019 yılında İBB'den ayrılan bazı personelden bağımsız olarak, Darkweb'e yüklenmiş olsun olmasın, inceleme konusu İBB verilerinin İBB sistemlerinden ele geçirilmediği, söz konusu verilerin bazı İBB çalışanlarının tek başlarına/bireysel olarak üye oldukları web sitelerinden *(örneğin sanalmuze.org)* ele geçirilmiştir. Her ne kadar e-mail adresleri @ibb.gov.tr uzantılı olsa da bu adres sadece bir kullanıcı adından ibarettir ve yalnızca belirlenen şifre ile kayıtlı sistemlerde çalışabilir.

İBB adına yüksek risk teşkil edebilecek tek durum, ilgili personelin İBB e-posta şifresini farklı sitelerde de kullanmasıdır ki bu durumda dahi siber korsanlar ancak şifresi sızan personelin e-postalarındaki bilgilere ulaşabileceklerdir.

5. Osint veya Darkweb'e koyulduğu belirtilen bu verilerin tek tek mi yoksa topluca mı ve kim tarafından yüklendiğini tespit etmek mümkün müdür?

Darkweb platformları, özellikle Tor ağı üzerinde çalışır. Bu mimari, veri yükleyen kullanıcıların IP adresini, fiziksel konumunu ve gerçek kimliğini bilinçli olarak gizlemek üzere tasarlanmıştır. Bu durum, Darkweb incelemelerini ele alan Avrupa Birliği Siber Güvenlik Ajansı (ENISA) raporlarında[34] açıkça vurgulanmıştır. Darkweb pazarları ve forumları verilerin ilk kaynaklarını kayıt altına almaz ve sızıntılar doğası gereği topluca yüklenir. Darkweb platformlarında genellikle kullanıcı logları tutulmaz; hatta tutulsa bile çoğunlukla sonradan silindiği kabul edilmektedir. "Collection", "Combo", "Dump" gibi adlarla paylaşılan veri setleri, kelime anlamlarından da anlaşılacağı üzere, genellikle uzun yıllar içerisinde farklı yerlerden sızmış

[31] https://mail.ibb.gov.tr/owa/auth/logon.aspx
[32] Microsoft Outlook'da şifreler en az 8 karakterli olmak zorundayken ekran görüntülerinde sızan 3 şifre de (2550as, 886777, Kiraz44) bu kritere uymamaktadır.
[33] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/
[34] Raporları: Fit for purpose *https://www.interface-eu.org/publications/enisa-fit-for-purpose*, New Mandate to Face Cyber Security Challenges https://ccdcoe.org/incyder-articles/enisas-new-mandate-to-face-cyber-security-challenges, Adapting ENISA's mandate and collaboration in a changing cyber landscape *https://www.digitaleurope.org/resources/adapting-enisas-mandate-and-collaboration-in-a-changing-cyber-landscape* Evaluation ENISA (European Union Agency for Cybersecurity) and the European Cybersecurity Certification Framework *https://onlinetrustcoalitie.nl/wp-content/uploads/2023/10/ENISA-and-EU-cybersecurity-cert-framework-evaluation-by-OTC-sept-2023.pdf*

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

milyonlarca kayıt barındırır. Çoğu zaman yükleyen kişi veriyi üreten veya ele geçirenler değil yeniden dağıtan kişi veya kişilerdir.

Bazı durumlarda veri ihlallerine neden olan sorumlular tespit edilebilmektedir, örneğin inceleme konusu e-posta adreslerinden i.basaran@ibb.gov.tr ve şifresini içeren veriyi sızdıran Polonya ve Ukraynalı iki fail, veri ihlalinin duyulma tarihinden 14 ay sonra yakalandıkları açıklanmış ancak gerçek isimleri kamuoyu ile paylaşılmamıştır[35].

6. Osint veya Darkweb'de bulunduğu iddia edilen bu verilere erişmek başlı başına illegal bir faaliyet midir? Bu verilere erişmek için hukuka aykırı bir yöntem kullanmak gerekir mi?

OSINT, hukuka uygun şekilde herkesin erişimine açık kaynaklardan bilgi toplama ve analiz etme faaliyetidir. Bu tanım gereği OSINT'te, yetkisiz erişim, teknik engel aşımı ve gizli sisteme girme gibi hukuk dışı olabilecek eylemler ilişkilendirilmez.

Hukuka aykırılık, veriye yetkisiz erişim sağlanması, teknik engel aşılması veya verinin suç teşkil edecek şekilde kullanılması hallerinde oluşabilecekken, dünya genelinde Darkweb'de sızdırılmış verilerin bulunması ve bu verilerin açık kaynaklardan incelenmesi, tek başına hukuka aykırı bir faaliyet olarak değerlendirilmemektedir..

Avrupa Birliği Siber Güvenlik Ajansı'na göre, OSINT ve Darkweb incelemeleri meşru analiz yöntemleri olarak kabul edilir. ABD Ulusal Standartlar ve Teknoloji Enstitüsü'ne (NIST) göre OSINT olay müdahalesinde ön analiz ve bağlamsal değerlendirme aracıdır. ISO/IEC 27043 standartlarında ise açık kaynak veriler destekleyici bulgu olarak kabul edilir.

7. Wickr isimli uygulama, Bylock uygulamasına benzer kapalı devre kriptolu bir program mıdır, açıklayınız?

Wickr, teknik olarak uçtan uca şifreleme kullanan bir haberleşme uygulaması olmakla birlikte, yine bir haberleşme uygulaması olan ByLock ile bir ceza yargılamasında aynı hukuki ve teknik kategoride değerlendirilmesinin yanıltıcı sonuçlar doğurabileceği anlaşılmaktadır.

Wickr, uçtan uca şifreleme (İng. end-to-end encryption) kullanan, bireysel ve kurumsal kullanıcılar için geliştirilmiş bir mesajlaşma uygulamasıdır[36].

Açık uygulama mağazalarından indirilebilir, herkes tarafından serbestçe kullanılabilir, bireysel, ticari ve kurumsal kullanım alanı vardır, Amazon Web Services bünyesinde, Wickr Me / Wickr Pro / Wickr Enterprise gibi farklı sürümleri bulunur ve şifreleme, genel kullanıcı gizliliği amacıyla tasarlanmıştır[37]. Wickr'de kullanıcı olmak için herhangi bir davet zinciri, kapalı devre kayıt sistemi veya örgütsel doğrulama mekanizması bulunmamaktadır.

ByLock, MİT'in (Milli İstihbarat Teşkilatı) ByLock Uygulaması Teknik Analiz Raporu'na[38] göre teknik olarak şifreli bir mesajlaşma uygulaması olmakla birlikte, hukuki değerlendirmesi teknik özelliklerinden ziyade kullanım biçimi üzerinden yapıldığı ve Wickr'a göre ayırt edici özellikleri

---

35 https://web.archive.org/web/20200521012054/https://ssu.gov.ua/ua/news/1/category/2/view/7602#.jnAqqCRr.dpbs

36 https://docs.aws.amazon.com/wickr/latest/adminguide/security.html

37 https://aws.amazon.com/wickr/

38 https://blog.fox-it.com/wp-content/uploads/2017/09/bylock-mit-technical-report-turkish.pdf

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

bulunduğu anlaşılmaktadır. Uygulamaya erişim kapalı devre şekilde sağlanmış, herkes tarafından serbestçe ve yaygın şekilde kullanılması mümkün olmamış, kullanıcı havuzu belirli bir yapı ile sınırlı kalmış ve yaygın sivil/kurumsal kullanım tespit edilmemiştir.

Yargıtay, ByLock hakkında verdiği yerleşik kararlarında "ByLock uygulaması, münhasıran FETÖ/PDY silahlı terör örgütü mensuplarının kendi aralarındaki iletişim için kullandıkları kapalı devre bir haberleşme programıdır." tespitini yapmıştır[39]. Bu kabulün dayanakları olarak; uygulamanın genel kullanıcı kitlesine hitap etmemesi, kullanımın örgüt içi haberleşme ile sınırlı kalması, başka bir meşru ve yaygın kullanım amacının ortaya konulamaması ve teknik verilerle desteklenen örgütsel bağı göstermiştir. Bu nedenlerle, Yargıtay'ın ByLock kararındaki ölçütler Wickr'e uygulandığında, Wickr'in ByLock ile aynı kapsamda değerlendirilmesi teknik açıdan doğru değildir.

8. Tarafınıza iletilen ifadelerde, Wickr isimli uygulamanın Hüseyin Gün ve müvekkilimiz Necati Özkan'a ait telefonlarda Adli Bilişim kıstasları dikkate alınarak yüklü olduğu tespit edilmiş midir?

Hüseyin Gün'ün ifadesi, kendi cihazında Wickr Me uygulamasını kullandığını açıkça gösterdiği anlaşılmaktadır. Şüpheli Hüseyin Gün ifadesinin devamında, Wickr uygulamasını App Store üzerinden indirdiğini ve WhatsApp'a kıyasla daha güvenli bulduğu için kullandığını beyan ettiği sabittir. Ayrıca Necati Özkan'a da Wickr uygulamasını indirmesini kendisinin önerdiğini belirtmiştir. Bu beyan, Hüseyin Gün'ün cihazında Wickr'in yüklü olup aktif kullanıldığını doğrular nitelikte görülmüştür. Nitekim ifadenin devamında kendi Wickr kullanıcı adını "Jupiter1881" olarak kullandığını da belirtmiş, bununla birlikte *"Hüseyin Gün isimli şüphelinin Wickr Me Kullanıcı Adının: Jupiter1881 – Giriş Şifresinin ise: sehergul1950 olarak kaydedilmiş olduğu"* açıkça görülmüş[40], sonuç olarak bu bilgiler, Hüseyin Gün'ün cihazında Wickr Me uygulamasının kurulu ve kullanılmış olduğu anlaşılmaktadır.

Necati Özkan'ın cihazlarında Wickr uygulamasının kurulup kurulmadığına ilişkin doğrudan bir dijital materyal inceleme sonucu tarafıma sunulan dosya içeriklerinde tespit edilememiştir. Necati Özkan'ın Wickr uygulaması kullandığı iddiası, Hüseyin Gün'ün telefonundan elde edilen WhatsApp yazışmaları arasında, 08 Ağustos 2019 tarihli bir mesajda "W'ye bak" (W'ye bak = "Wickr'e bak") şeklinde yer alan bir ifade kaynaklı olduğu anlaşılmaktadır.

Wickr uygulaması, kullanıcılara takma ad (rumuz) ile hesap oluşturarak anonim iletişim imkânı veren, uçtan uca şifreli bir mesajlaşma uygulamasıdır. Uygulama, uçtan uca şifreleme ve anonim hesap yapısı nedeniyle merkezi sunucularda kullanıcı kimlik bilgisi veya içerik barındırmamaktadır. Herhangi bir telefon numarası veya gerçek kimlik doğrulaması zorunlu değildir; kullanıcılar istedikleri bir rumuz ile hesap açabilirler. Bu nedenle, bir Wickr kullanıcı adını doğrudan gerçek bir kişiye ait olduğunu doğrulamak, platformun doğası gereği kendiliğinden mümkün değildir. Adli bilişim açısından, bir Wickr rumuzunun belirli bir şahsa ait olduğunu göstermek için cihaz içi verilerden elde edilecek kanıtlara ihtiyaç duyulur. Bu nedenle adli bilişim uzmanları, kimlik atamasını cihazlardaki izlere ve verilere dayandırmak zorundadır. Eğer böyle dolaylı veriler mevcut değilse, sadece bir Wickr kullanıcı adına bakarak onun hangi şahsa ait olduğunu kesin olarak söylemek mümkün olmaz.

---

[39] https://www.kazanci.com.tr/gunluk/16cd-2019-11650.htm
[40] Hüseyin Gün Şüpheli İfade Tutanağı, Sayfa 152

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754666, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

9. *Soruşturma kapsamındaki şüphelilerden Hüseyin Gün'ün açık kaynaklarda yer alan Emniyet ifadesinin, 194 ve 195. sayfalarında ve Hüseyin Gün'e ait olduğu iddia edilen mesajda ve "Bu haberlerin etkisi görünürlüğü azaltılabilir mi?" ve "O dönemde yapay zeka dijital ordu" söylemlerinden anlatılmak istenen nedir?*

Hüseyin Gün'e ait ifadenin 194. ve 195. sayfalarında yer almış ve kendisine ait olduğu iddia edilen mesajlar üzerinde yapılan araştırmalarda, mesaj içeriklerinin 2019 yılı İstanbul Büyükşehir Belediyesi seçimleri sonrasında yaşanan veri tabanı kopyalama tartışmaları bağlamında dile getirildiği, ifadeyi veren Hüseyin Gün'ün, belediye seçim kampanyası döneminde dijital yöntemlerle olumsuz haberleri bastırmaya yönelik bir girişimde bulunduğunu beyan ettiği anlaşılmaktadır[41].

Yapılan incelemelerde, "yapay zeka dijital ordu" kavramı ve "haberlerin bastırılması / görünürlüğünün azaltılması" eylemlerinin bir arada tanımlandığı anlaşılmaktadır. Bu durumda, söz konusu kavramların teknik, operasyonel ve psikolojik anlamlarının birlikte analiz edilmesi gerekir. Konuyla ilgili olarak tarafımca, yalnızca uzmanlık alanlarım dahilindeki siber operasyonlar, sosyal medya manipülasyonu, görünürlük (içerik) bastırma, algoritmik yönlendirme ve bot/trol ağları gibi teknik ve operasyonel olgularla ilişkisine cevap verilebilir niteliktedir.

"**Dijital ordu**", genel anlamıyla koordineli bir dijital hesaplar topluluğunun (bot hesaplar, sahte profiller veya organize gerçek kullanıcı grupları) belirli bir amaç doğrultusunda, eşgüdümlü şekilde hareket etmesini ifade eder. Bu kavram, özellikle sosyal medya platformlarında belirli içerikleri yaygınlaştırmak veya bastırmak, algı oluşturmak ve kamuoyu manipülasyonu yapmak için kullanılan geniş çaplı hesap ağlarını anlatır. Bu ağlar, insan operatörler tarafından yönetilebildiği gibi otomasyonla (bot yazılımlarıyla) da yönetilebilir. "Yapay zekâ dijital ordu" ifadesi ise bu bot/trol ağlarının daha gelişmiş, yapay zekâ destekli sürümünü ima etmektedir. Yani, sıradan botların ötesinde, yapay zekâ algoritmaları ile yönetilen veya içerik üreten bir dijital hesaplar ordusu söz konusudur.

Teknik açıdan, böyle bir dijital ordu binlerce hesabı veya cihazı tek merkezden yönetebilen yazılımlar ve altyapılar gerektirir. Örneğin, literatürde ve uygulamada bot çiftliği (İng. bot farm) veya telefon çiftliği (İng. phone farm) denen yapılar bulunmaktadır. Bunlar, bir oda dolusu fiziksel cihazın (akıllı telefon, bilgisayar vb.) özel yazılımlarla kontrol edilerek, sanki her biri gerçek bir kullanıcıymış gibi davranmasını sağlar[42].

Yapay zeka ise bu süreçte, bot hesapların daha inandırıcı davranması, içeriklerin otomatik olarak üretilmesi *(örneğin gerçek insanların yazdığına benzer gönderiler, yorumlar*) veya hedeflenen mesajların doğru kitlelere ulaştırılması için kullanılabilir. 2019 yılı itibariyle bu tür Yapay Zeka destekli bot teknolojileri henüz yaygınlaşmamış olsa da, konsept olarak mevcut olduğu ve bazı gelişmiş siber operasyon birimlerince kullanıldığı bilinmektedir.

Hüseyin Gün'ün ifadesinde, dijital ordunun aktif hale getirilmesinden bahsedildiği anlaşılmaktadır. Eğer gerçekleşmişse, benzeri bir operasyon; İBB veri kopyalama haberleri ile

---

[41] Hüseyin Gün Emniyet İfadesi 194 ve 195. sayfalar ayrıca açık kaynaklarda yapılan araştırmalar. (*https://www.aydinlik.com.tr/haber/huseyin-gunun-ozkana-attigi-mesaj-veri-tabani-kopyalama-risklerini-azalttik*)

[42]Telefon Çiftlikleri – Dijital Kölelikten Algı Savaşına, Halil İbrahim Büyükbaş, Stratejik Düşünce Enstitüsü *https://www.sde.org.tr/halil-ibrahim-buyukbas/genel/telefon-ciftlikleri--dijital-kolelikten-algi-savasina-kose-yazisi-61192*

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

ilgili çok sayıda içerik üretmek veya paylaşmak, koordineli hesaplar ağı kullanarak, aynı anda veya kısa süre içinde bu içerikleri yaymak, algoritmik yönlendirme taktikleri uygulamak ve gerekirse içerik şikayeti/raporlama faaliyetleri şeklinde gerçekleştirilebilir. Ayrıca bu süreç, iyi planlanmış bir sosyal mühendislik ve teknik altyapı gerektirir.

Özetle, "yapay zeka dijital ordu" ifadesi hem ileri düzey teknik bir enstrümanı, hem de bir siber algı operasyonunu tanımlamaktadır. Böyle bir ordunun varlığı durumunda geride kalabilecek dijital izler (örn. aynı anda benzer içerik paylaşan binlerce hesap, IP/proxy izleri, anormal etkileşim grafikleri gibi) analiz edilebilir. Bununla birlikte, aradan geçen zaman, varsa bu tip ağların izlerini gizlemek için dağıtık ve yabancı altyapılar kullanması ve sosyal medya platformlarının log kayıtlarına ulaşılamaması gibi nedenlerle yapılacak analiz sonucu güvenilir, kesin ve net olmayacaktır.

"Haberlerin etkisinin görünürlüğünü azaltmak" ifadesi, dijital platformlarda yayılan belirli haberlerin daha az kişiye erişmesini sağlamak veya habere maruz kalan kişilerin algısındaki etkisini düşürmek anlamlarına gelir. Teknik olarak, doğrudan bir silme veya sansüründen farklı olup, daha incelikli içerik bastırma (İng. content suppression) stratejisi anlamında kullanılmış olabilir.

Teknik olarak böyle bir operasyonun yapılabilmesi için muhtemelen; arama motoru optimizasyonları (SEO) ile haberlerin görünürlüğünü azaltma, sosyal medya trendlerini farklı içeriklerle bastırma, haber kaynaklarına organize şekilde olumsuz tepki verme ve alternatif gündem yaratma gibi adımları içerebilir.

SONUÇ

İşbu uzman mütalaası, belirtilen kapsam çerçevesinde teknik uzmanlık ve adli bilişim bilgileri doğrultusunda tarafsız olarak hazırlanarak, hiçbir baskı veya etki altında kalmadan, ekleri ile birlikte 18 sayfa, tek nüsha olarak hazırlanmış ve 5070 sayılı kanun gereğince güvenli elektronik imza ile imzalanarak sunulmuştur. (5 Şubat 2026)

Tuncay Beşikçi

Adli Bilişim Mühendisi (1. Sınıf Onur Derecesi, Middlesex University, Birleşik Krallık)
Adli Bilirkişi (2013-2018, İstanbul Ceza ve Hukuk Mahkemeleri No:7824)
Avrupa Birliği – Sertifikalı Siber Adli Bilişim Profesyoneli (CCFP-EU No:440505)

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754696, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

EK 1 – TALEP YAZISI

ERDEM AVUKATLIK BÜROSU

Sayın Tuncay Beşikçi'nin Dikkatine,

05.11.2025

Müvekkilimiz Necati Özkan hakkında, İstanbul Cumhuriyet Başsavcılığı nezdinde 2025/57354 Sor. numaralı soruşturma yürütülmektedir.

5271 sayılı Ceza Muhakemesi Kanunu'nun 67. maddesinin 6. fıkrası kapsamında "uzman kişinin bilimsel mütalaası" olarak yukarıda bahsedilen soruşturma dosyasına sunulmak üzere, tarafınızca, sizlere sunmuş olduğumuz ifadeler ve belgeler dikkate alınarak ve tarafınızca yapılacak araştırmalar neticesinde, aşağıda ayrıntılı olarak belirtilen soruları yanıtlar biçimde bir uzman mütalaası hazırlanmasını talep ediyoruz:

1. Soruşturma kapsamında geçen Osint ve Darkweb kavramları nedir?
2. Soruşturma kapsamındaki şüphelilerden Hüseyin Gün'ün açık kaynaklarda yer alan Emniyet ifadesinin, 124 ve 125. sayfalarında geçen ve İstanbul Büyükşehir Belediyesi'ne ait olduğu iddia edilen veriler nelerdir?
3. Darkweb'den alındığı belirtilen bu veriler yine 125. sayfada yer alan ekran görüntüsü uyarınca, hangi anahtar kelime ya da kelimeler aratılarak bulunmuş, spesifik bir isim ya da bilgi girilmiş midir?
4. Yine bu kapsamda İBB'den alınan ve ekte sunulan cevabi yazı uyarınca, suçlama konusu yapılan İBB personellerinin e-posta adres ve şifreleri dikkate alınarak, bu kişilerden bazılarının 2019 yılından önce İBB'den ayrıldıkları değerlendirildiğinde, bu kişilerin e-posta ve şifrelerinin 2019 yılı itibarıyla Darkweb'te yer almasının bir önemi bulunmakta mıdır, bu kişilerin e-posta ve şifreleri hangi yılda Darkweb'e yüklenmiş olabilir?
5. Osint veya Darkweb'e koyulduğu belirtilen bu verilerin tek tek mi yoksa topluca mı ve kim tarafından yüklendiğini tespit etmek mümkün müdür?
6. Osint veya Darkweb'de bulunduğu iddia edilen bu verilere erişmek başlı başına illegal bir faaliyet midir? Bu verilere erişmek için hukuka aykırı bir yöntem kullanmak gerekir mi?
7. Wickr isimli uygulama, Bylock uygulamasına benzer kapalı devre kriptolu bir program mıdır, açıklayınız?
8. Tarafınıza iletilen ifadelerde, Wickr isimli uygulamanın Hüseyin Gün ve müvekkilimiz Necati Özkan'a ait telefonlarda Adli Bilişim kıstasları dikkate alınarak yüklü olduğu tespit edilmiş midir?
9. Soruşturma kapsamındaki şüphelilerden Hüseyin Gün'ün açık kaynaklarda yer alan Emniyet ifadesinin, 194 ve 195. sayfalarında ve Hüseyin Gün'e ait olduğu iddia edilen mesajda ve "Bu haberlerin etkisi görünürlüğü azaltılabilir mi?" ve "O dördünde yapay zeka dijital ordu" söylemlerinden anlatılmak istenen nedir?

Tarafınızca hazırlanacak olan uzman mütalaasının 3 (üç) nüsha olarak hazırlanmasını ve ıslak imzalı suretlerin tarafımıza iletilmesini, arz ve talep ederiz.

Saygılarımızla,

Necati Özkan

Müdafii

Av. Erkam Erdem

TUNCAY BEŞİKÇİ

Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864734866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

EK 2 – YASAL DAYANAK

İşbu Uzman Mütalaası, aşağıda belirtilen kanun maddeleri ve Yargıtay İlke Kararı kapsamında tanzim edilmiştir.

5271 SAYILI CEZA MUHAKEMESİ KANUNU

CMK Md. 67/6, Cumhuriyet savcısı, katılan, vekili, şüpheli veya sanık, müdafii veya kanunî temsilci, yargılama konusu olayla ilgili olarak veya bilirkişi raporunun hazırlanmasında değerlendirilmek üzere ya da bilirkişi raporu hakkında, uzmanından bilimsel mütalaa alabilirler. Sadece bu nedenle ayrıca süre istenemez.

6100 SAYILI HUKUK MUHAKEMELERİ KANUNU

HMK Md. 266/(1) Mahkeme, çözümü hukuk dışında, özel veya teknik bilgiyi gerektiren hâllerde, taraflardan birinin talebi üzerine yahut kendiliğinden, bilirkişinin oy ve görüşünün alınmasına karar verir. Hâkimlik mesleğinin gerektirdiği genel ve hukuki bilgiyle çözümlenmesi mümkün olan konularda bilirkişiye başvurulamaz.

HMK Md. 293

(1) Taraflar, dava konusu olayla ilgili olarak, uzmanından bilimsel mütalaa alabilirler. Sadece bu nedenle ayrıca süre istenemez.

(2) Hâkim, talep üzerine veya resen, kendisinden rapor alınan uzman kişinin davet edilerek dinlenilmesine karar verebilir. Uzman kişinin çağrıldığı duruşmada hâkim ve taraflar gerekli soruları sorabilir.

(3) Uzman kişi çağrıldığı duruşmaya geçerli bir özrü olmadan gelmezse, hazırlamış olduğu rapor mahkemece değerlendirmeye tabi tutulmaz.

HMK Md. 284 / (1) Bilirkişi, Türk Ceza Kanunu anlamında kamu görevlisidir.

YARGITAY İLKE KARARI

Yargıtay Ceza Genel Kurulu 9.10.2007 Tarih, 2006/7-336 Esas, 2007/198 Karar Sayılı ilke kararı ilgili bölümü: "Soruşturma ve kovuşturma makamlarınca derlenmiş bilirkişi mütalaaları ile tarafların kendi girişimleriyle aldırmış oldukları özel bilimsel görüşlerin duruşma evresinde tartışılma ve değerlendirilmesi usulünün farklı olmayıp aynı hükümlere tabi bulunduğu gözetilmeyerek (…) ilk hükmün tefhim edildiği oturumda, kişilerin kendi girişimleriyle düzenlettirildiği anlaşılan bilimsel görüşün sahibinin uzman tanık olarak dinlenmesi sonrasında, serdedilen görüşe karşı diyeceklerini bildirmek üzere süre isteyen sanık müdafilerinin bu istekleri ile ilgili olarak makul süre tanımak ve 5271 sayılı CMK'nun 67/6, 68/3, 214/3, 215, 216 ve 217'nci maddelerince değerlendirme yapmak gerekirken, savunma hakkını kısıtlayacak biçimde istemin reddine hükmedilmesi ve bu konudaki bozma kararına usule aykırı gerekçelerle direnilmesi isabetli görülmemiştir."

Yargıtay 15. Hukuk Dairesi, 10.11.2016 tarih, 2015/5127 E. ve 2016/4635 K. Sayılı kararında, mahkemece yapılan bilirkişi incelemesi neticesinde ortaya çıkan bilirkişi raporu ile taraflardan biri tarafından dosyaya sunulan uzman görüşü arasında çelişkiler bulunması halinde, çelişkilerin giderilmesi amacıyla dosyanın "yeni bir bilirkişi heyetine" tevdii edilmesi gerektiğine hükmetmiş ve bunun gerekçesi olarak, uzman görüşü sunan tarafın adil yargılanma hakkının ihlali oluşabileceğine vurgu yapmıştır: (...) "Dava, eser sözleşmesinden kaynaklanan ayıplı imalat nedeniyle doğan alacağın tahsili istemine ilişkindir. Dosyada alınan bilirkişi raporuna, taraflardan biri, uzman görüşüne dayanmak suretiyle itiraz etmiş ve bu itirazlar mahkeme tarafından hiç değerlendirmeye alınmamış ve itirazlar gerekçeli bir şekilde karşılanmamış ise, uzman görüşüne dayanan tarafın 6100 sayılı HMK'nın 27., Anayasa'nın 36. ve Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesinde düzenlenen adil yargılanma hakkının en önemli unsuru olan hukuki dinlenme hakkını ihlal etmiş olabilecektir. Dosyaya ibraz edilen uzman görüşünde bilirkişi raporu ile tespit edilen görüşlerinin aksine tespit ve görüşler ileri sürülmüş olup, bilirkişi raporu ile uzman görüşü ciddi şekilde çelişkiler içermektedir. Alınan bilirkişi raporu ile uzman görüşü arasındaki çelişkinin giderilmesi amacıyla dosyanın yeni bir bilirkişi heyetine tevdii edilmesi yerine yetersiz ve esaslı itiraza uğrayan rapora dayanılarak uzman görüşü kararda gerekçeli olarak değerlendirilip tartışılmadan karar verilmiş olması doğru olmamış, bozmayı gerektirmiştir. ...Alınan bilirkişi raporuna davalı vekili esaslı itirazlarda bulunmuş ve bu itirazlarına 6100 sayılı HMK'nın 293.maddesi gereğince alınan uzman görüşünü dayanak olarak eklemiştir. Bilindiği üzere 6100 sayılı HMK'nın 293. maddesinde düzenlenen uzman görüşü, tarafların uyuşmazlığın aydınlanabilmesi, anlaşılabilmesi ve iddia ve savunmaların ispatı için kendisinin belirlediği özel ve teknik bilirkişiden bir konuda bilgi alması olarak düzenlenmiş olup, uygulamada özel bilirkişi adı da verilmektedir. Taraflar kendi menfaatlerini koruyabilmek ve alınan bilirkişi raporundan tatmin olmamaları halinde olayın tam olarak aydınlanmasını sağlamak ve doğru ve adil kararın verilmesi için uzman görüşü alıp mahkemeye ibraz edebilecektir. Mahkeme özellikle özel ve teknik bilgiyi gerektiren konularda, tarafın sunduğu uzman görüşünün dava konusuyla ilgili olması halinde mutlaka dikkate almak ve değerlendirmek zorundadır. .... Alınan bilirkişi raporu ile uzman görüşü arasındaki çelişkinin giderilmesi amacıyla dosyanın yeni bir bilirkişi heyetine tevdii edilmesi yerine yetersiz ve esaslı itiraza uğrayan rapora dayanılarak uzman görüşü kararda gerekçeli olarak değerlendirilip tartışılmadan karar verilmiş olması doğru olmamış, bozmayı gerektirmiştir.

Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754866, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0

EK 3 – UZMAN KİMLİĞİ

Tuncay Beşikçi, 1977, İstanbul

Londra Middlesex Üniversitesi, Mühendislik ve Bilgi Bilimleri Fakültesi, Adli Bilişim Mühendisliği bölümünden 1. Sınıf Onur Derecesi ile bölüm birincisi olarak mezun olmuştur.

Adli Bilişim, Bilgi Güvenliği, Olay Yeri İncelemesi, Zararlı Yazılım Analizi, Veri Sahteciliği ve Hırsızlığı, Sızma Testleri, Bilişim Suçları, Siber Savunma, Veri ve Şifre Kurtarma, İşletim Sistemleri, Mobil Cihazlar ve İnternet Adli İncelemesi gibi konularda; aralarında Emniyet İstihbarat Daire Başkanlığı, Siber Suçlarla Mücadele Daire Başkanlığı, Polis Kriminal Büro, Adli Tıp Kurumu ve Jandarma Kriminal Büro gibi kamu ve özel sektörden birçok kuruluşa eğitmenlik ve danışmanlık hizmetleri sunmuştur.

2012 yılı öncesinde Birleşik Krallık'da 10 yıl süre ile bilişimin; veritabanları, programlama, bilgisayar ve ağ güvenliği gibi çeşitli alanlarında çalışmış, İngiliz Yüksek Mahkemesi'nde (Royal High Court of Justice) bilirkişilik yapmış ve Londra Polis Teşkilatı'nın Elektronik Suçlar Bölümü'nde (London Metropolitan Police e-Crime Unit) yaptığı incelemelerle çok sayıda adli davanın çözümlenmesine katkı sağlamıştır.

2013 ve 2017 yılları arasında İstanbul Adliyesi Hukuk ve Ceza Mahkemeleri'nde Adli Bilişim, Bilişim, İnternet ve Sahtecilik Suçları gibi konularda kayıtlı Adli Bilirkişidir. Bu kapsamda özellikle dijital delillerin davaların seyrini belirlediği, kamuoyunda Balyoz, Poyrazköy, Atabeyler, OdaTV, 28 Şubat, Askeri Casusluk ve FETÖ/PDY adları ile bilinen davalarda mahkeme tarafından görevlendirilerek bilirkişilik yapmış ve bilimsel uzman mütalaaları hazırlamıştır.

27 Aralık 2017 tarihinde Ankara Cumhuriyet Başsavcılığı'nca açıklanan ve kamuoyunda 'Morbeyin Kumpası' olarak bilinen FETÖ tuzağının ortaya çıkarılmasında Savcılık ve devlet bünyesinde oluşturulan teknik ekiple birlikte çalışmış, tuzağın arkasındaki FETÖ ilişkili şahsı tespit etmiş, Namaz/Kıble cep telefonun uygulamalarının kullanıcıları ByLock sunucusuna yönlendirdiğini bilimsel olarak kanıtlamış ve tuzağa düşüp yargılanmakta olan en az 11,480 kişinin tahliye olmasına katkı sağlamıştır.

BCS (British Computer Society), ACFE (Association of Certified Fraud Examiners), INETA (International .Net Association), (ISC) 2 (International Information Systems Security Certification Consortium, Inc.) ve Adli Bilişim Derneği üyesidir. Raporun yazıldığı tarihte dünya genelinde 49 kişinin sahip olduğu, tüm Avrupa Birliği ülkelerince kabul edilen, Adli Bilişim ve Siber Güvenlik alanlarında en üst düzey sertifikalardan biri olan CCFP-EU (Certified Cyber Forensic Professional - European Union) ünvanlı Türkiye'deki ilk ve tek kişi olması haricinde Accessdata, Guidance Software, Microsoft, Ec-Council, Ace Laboratory ve Cisco gibi firmalardan bilişimin çeşitli alanlarında çok sayıda sertifika sahibidir. İyi derecede İngilizce bilmektedir.

Bilirkişi olarak görevlendirildiği davalardan bazıları şöyledir:

- 2014/128199, FETÖ/PDY iltisaklı Poyrazköy Kumpası Davası
- 2015/48932, Oslo Görüşmelerinin Sızdırılması
- 2015/91043 DHKPC mensubu kişide Başbakan Erdoğan'ın ev krokisinin bulunması
- 2012/653, FETÖ/PDY Telekom yapılanması
- 2015/20679, FETÖ/PDY iltisaklı usulsüz telefon dinlemeleri
- 2014/124746, F. Gülen'i araştıran gazeteci Haydar Meriç cinayeti
- 2017/148, Cumhuriyet Gazetesi Davası
- 2024/396, Narin Güran Cinayeti Davası

Görev aldığı uluslararası davalardan bazıları:

- Amerika – 4D2022-0615, Tatlici v Tatlici (2023) – District Court of Appeal of Florida, Fourth District
- Birleşik Krallık – R v Paul Davies (2013) – Pub murder of M. O'Reilly (Analysis of call data)
- Birleşik Krallık – R v Wayne COUZENS (2021) – Murder of Sarah Everard
- Ukrayna – 2020 Ukravtodor v EBRD and the European Investment Bank

TUNCAY BEŞİKÇİ
Digitally signed by TUNCAY BEŞİKÇİ
DN: SERIALNUMBER=46864754666, C=TR, L=İSTANBUL, CN=TUNCAY BEŞİKÇİ
Reason: your signing reason here
Location: your signing location here
Date: 2026.02.05 21:33:27+03'00'
Foxit PDF Editor Version: 2024.1.0