T.C.
İSTANBUL
25. AĞIR CEZA MAHKEMESİ

DOSYA NO : 2026/55 Esas
BAŞKAN : Necati Sezer ÇÜMEN 139814
ÜYE : Gizem TULĞAY 215439
ÜYE : Melike İkra UĞUZ 233961
KATİP : Raif SİNİRLİOĞLU 221362

BİLİRKİŞİ RAPORU

GÖREVLENDİRME: İddianamede atılı suç kapsamında ele geçirildiği iddia edilen veriler ile ilgili olarak *bahsi geçen verilerin ibb.gov.tr veri tabanından ele geçirilip geçirilmediği, anılan veri tabanından ele geçirildi ise ne şekilde (hackleme/sızma) hangi tarihte ele geçirildiği, *iddianame anlatımında geçen OSINT ve DARKWEB ifadeleri gözetildiğinde bu verilerin atılı suç tarihi öncesinde internet ortamına sızmış veriler olup, olmadığı, sızdı ise bu verilerin hangi tarihte ne şekilde internet ortamına sızdığı, bu verilerin internetin kamuya açık alanlarında bulunup bulunmadığı hususlarında inceleme yapıp,
Dosyada yer alan iddianame ile sanık Hüseyin GÜN'ün 26/10/2025 tarihli kolluk ifadesinin 123., 124. Ve 125. Sayfalarında yer alan ekran görüntülerinin bilirkişiye verilmesi.

TESLİM ALINAN MATERYALLER:
Görevlendirme kapsamında tarafıma sadece bir adet ELBA marka 700 MB kapasiteli CD-R optik medya teslim edilmiştir. İlgili optik medya içeriği aşağıdaki gibidir.

123. Sayfa.jpg	19.02.2026 13:24	JPG File	1.781 KB
124. Sayfa.jpg	19.02.2026 13:24	JPG File	1.487 KB
125. Sayfa.jpg	19.02.2026 13:24	JPG File	1.811 KB
İddianame kapak.udf	19.02.2026 13:29	UDF File	13 KB
İddianame.tif	19.02.2026 13:27	TIFF image	12.344 KB

ÖNEMLİ BİLGİLENDİRME 1 : Rapor içerisinde kaynak gösterilen bilgiler açık kaynak verilerden, kamu kurum ve kuruluşları internet sitelerinden, görevlendirme ve rapor teslim tarih aralığında erişim sağlanan bilgilerdir.

ÖNEMLİ BİLGİLENDİRME 2 : İş bu rapor görevlendirme kapsamında iddianame nazara alınarak hazırlanmıştır. Kanunlar kapsamında raporun elde edilerek, bir bölümünün alıntılanarak kullanılması; rapor bütünlüğünün bozulmasına, farklı değerlendirme ve anlamlandırmalarla kullanılabileceği dikkate alınması, her dosya, içerisindeki delil ve iddialarla değerlendirilmesi ilkesi çerçevesinde iş bu raporun bir bölümünün ya da tamamının kullanılması yanıltıcı olabileceği dikkate alınması, kullanıldığı takdirde yok hükmünde sayılması gerektiği ilgili makamlardan arz ve talep olunur.

"BİLİRKİŞİ RAPORUDUR."

BİLİRKİŞİ RAPORU
BÖLÜM-1
GENEL BİLGİLER

Bu rapor, teknik içerik barındırması nedeniyle üç ana bölüm halinde yapılandırılmıştır.

Birinci bölümde, bilgi teknolojileri alanına ilişkin kavram ve konular genel çerçevede ele alınarak raporun bütünlüğünün anlaşılmasına katkı sağlanması amaçlanmıştır.

İkinci bölümde, görevlendirme kapsamında incelenen verilerin teknik analizi yapılmış, gerçekleştirilen çalışmalar sistematik biçimde ortaya konulmuştur.

Üçüncü ve son bölümde ise birinci ve ikinci bölümde sunulan bulgular ışığında elde edilen sonuçlar bilimsel ve tarafsız bir yaklaşımla değerlendirilmiş; nihai takdir Sayın Mahkeme Heyetine aittir. Başlıklar aşağıdaki gibidir.

Siber Uzay (Cyberspace) Kavramı

Siber Güvenlik

Siber Uzay Kaynakları ve Dijital Varlıklar

Türkiye'de Siber Güvenlik Çalışmaları ve Kurumsal Yapılanma

Tehdit Aktörleri ve Hacker Profilleri

Veri Sızıntısı (Data Leak / Data Breach)

Darknet ve Dark Web Kavramları

Dark Web İçerik Ekosistemi

Siber Tehdit İstihbaratı (Cyber Threat Intelligence – CTI)

Açık Kaynak İstihbaratı (Open Source Intelligence – OSINT)

Yaygın Kimlik Doğrulama Alışkanlıkları ve Parola Güvenliği

A- SİBER UZAY (CYBERSPACE) KAVRAMI

1. ***İsim, bilişim*** **Genel ağa ait olan:**
   "*Uydu ve siber iletişim dünyasında meydana gelen bu değişimden sonra internet hayatın tüm alanları için kullanılabilir bir araca dönüştürüldü"* - Murat Orçan
2. ***isim*** **Bilgisayara ait olan.**

Kaynak: https://sozluk.gov.tr/

Ağ kavramı, herhangi bir iletişim altyapısı üzerinden birbirine bağlanabilen cihazları ve bu cihazların oluşturduğu bağlantı yapısını ifade eder. Birbirine bağlı tüm ağların küresel ölçekteki bütününe ise internet adı verilmektedir. Günümüzde cihazlar, ağlar ve kullanıcıların etkileşim içinde bulunduğu dijital ortam, Siber Uzay (Cyberspace) olarak tanımlanmaktadır.

B- SİBER GÜVENLİK

Siber uzayda bulunan kişisel veriler, şirket verileri, devlet sistemleri, sunucular, ağ altyapıları, mobil cihazlar ve IoT (Nesnelerin İnterneti – ağa bağlanabilen cihazlar) gibi dijital varlıkların güvenliğinin sağlanması, siber güvenliğin temel kapsamını oluşturmaktadır.

C- SİBER UZAY KAYNAKLARI VE DIJITAL VARLIKLAR

Siber Uzay içerisinde bulunan kaynaklar genel olarak iki sınıfta değerlendirilebilecektir. Bunlar, Açık kaynak ve kapalı kaynak olarak adlandırılmaktadır.

1. **Açık Kaynak:** Herkesin yasal olarak erişebildiği, gizli olmayan dijital kaynaklardan elde edilen verilerdir.

2. **Kapalı Kaynak:** Yasal olarak erişmeye yetkisi olan kişilerin bilmesi gerektiği prensibi ile sınırlı erişim ile erişilebilir bilgilerin olduğu alanlardır. Bu alanlar kendi içlerinde de ayrışabilmektedir. Güvenlik kurallarına göre tamamen kapalı olmakla birlikte kurumların ilgili verileri de bu kapsama girebilecektir.

   Kamu Kurumları kapsamında değerlendirildiğinde tamamen kapalı kaynaklar Kara Kuvvetleri Komutanlığına ait "KARANET", Hava Kuvvetleri Komutanlığı "HAVANET" ve benzeri bir sistem olan Emniyet Genel Müdürlüğü'nün POLNET sistemleridir. Bu sistemler tamamen kapalı sistemlerdir.
   Millî Savunma Bakanlığı (MSB) ile çalışacak kurumların da kaynaklarına erişimi sınırlandırılmaktadır. Oluşturulacak bilişim ağlarına ilişkin de TÖGEK (Tesis Özel Güvenlik El Kitabı) içerisinde;
   "BÖLÜM 11 BİLGİ SİSTEMLERİ İÇİN ALINAN ÖNLEMLER bilgisayarlar, çevre birimleri, telefon ve enerji hatları, elektronik güvenlik sistemleri ve network yapılanması ile ilgili tüm uygulama, kural ve işlemler gizlilik dereceli işlere göre yapılandırılmıştır. Yapılanmada "kırmızı" ve "siyah" olmak üzere iki çeşit mimari belirlenmiştir. Kırmızı ve siyah hatlar standart kablo ile döşenmişse aralarında yansımayı önlemek maksadıyla 15 cm mesafe bırakılmıştır. Bu mesafenin bırakılmasına, fiber kablo kullanılması durumunda gerek yoktur. ÖZEL ve üzeri gizlilik dereceli bilgilerin yer aldığı bilgisayar/yazılım sistemi için yansıma (TEMPEST) tedbirleri alınacaktır."
   Kaynak:
   https://www.msb.gov.tr/content/upload/docs/TekHizDSavSanGuv/T%C3%96GEK160320.docx

   Kısaca MSB TÖGEK içerisinde Kırmızı ağ (kapalı/gizli/tesis) ve siyah ağ (açık/internet) olarak sınıflandırmaktadır. Diğer kamu kurumları ve ticari şirketlerinde sınıflandırdığı bilgiler kapalı kaynak olarak değerlendirilecektir. Bu ağlardaki verilerde güvenlik duvarları ve benzeri koruma teknolojileri ile korunan sistemlerde yine kapalı kaynak olarak değerlendirilebilecektir.
   Özetle kapalı bir ağa <u>yetkisiz erişim</u> bir kurum/kuruluş çalışanı ya da internet üzerinden erişen (Hacker/tehdit aktörü) olması durumunda suç teşkil edecektir.

Herhangi bir kurum ya da ticari kuruluş verilerinin belirli bir kısmı da gerekli teknik tedbirler alınarak erişmeye yetkisi olan kişiler tarafından erişilmesine izin verilmektedir. Örneğin, bir kişinin bilişim sistemleri marifetiyle bir bankanın sistemindeki kendi verilerine yetkileri çerçevesinde erişmesi hayatın olağan akışında kabul edilebilir bir durumdur. Dosya kapsamındaki İBB'nin de kamu hizmeti çerçevesinde ilgili teknik tedbirleri alarak ilgililerine kapalı kaynak olan verileri ilgisine açmak (Vergi/borç ödemeleri vb.) hayatın doğal akışına uygundur. Bu erişimlerin tamamı iş ve işleyişleri, yasal sorumlulukları yerine getirmek için yasal olarak farklı kurumlarla da paylaşılabilecektir.

D- TÜRKİYE'DE SİBER GÜVENLİK ÇALIŞMALARI VE KURUMSAL YAPILANMA

1. 6659 sayılı Kişisel Verilerin Korunması Kanunu

24 Mart 2016 tarihinde Türkiye Büyük Millet Meclisinde kanun kabul edilmiştir. Kanun, kişilerin verilerinin güvenliğini sağlamakla ilgili olarak yürürlüğe girmiştir. İlgili kanunla Kişisel Verileri Koruma Kurumu kurulmuştur. Kurumun belirlediği kriterleri sağlayan tüm kamu ve özel kurumlar (Şirketler) kuruma karşı yükümlülükleri bulunmaktadır. Çalışan, üye, paydaş ve sair tanıma uyan herhangi bir gerçek ve tüzel kişilerin verileri iş bu kanun çerçevesinde kişisel veri kabul edilmektedir.

İş bu dosya kapsamında ilgili kanunun önemi **Veri İhlali** olması durumunda kriterlere uyan kamu ya da şirketlerin ihlali bildirme yükümlülüğü bulunmasıdır.

2. USOM (Ulusal Siber Olaylara Müdahale Merkezi)

20/10/2012 tarih ve 28447 sayılı Resmi Gazete'de yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince 20/06/2013 tarih ve 28683 sayılı Resmi Gazate'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı ile "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" kapsamında, Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur.

Ayrıca 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulmuştur. USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları öncelemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır. USOM ile Kurumsal SOME ve/veya Sektörel SOME'nin koordineli çalışması ve işbirliği halinde olması ulusal siber güvenliğimize katkı sağlamaktadır.

USOM, ülkemizdeki siber olaylara müdahale konusunda ulusal ve uluslararası koordinasyon çalışmaları 7/24 çalışma esasına göre yürütülür. Bu kapsamda yapılan çalışmalarda tespit edilen siber tehditlerle ilgili olarak ilgili taraflara ya da ülke çapında alarm, uyarı ve duyurular yaparak yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesini sağlar. Siber güvenlik

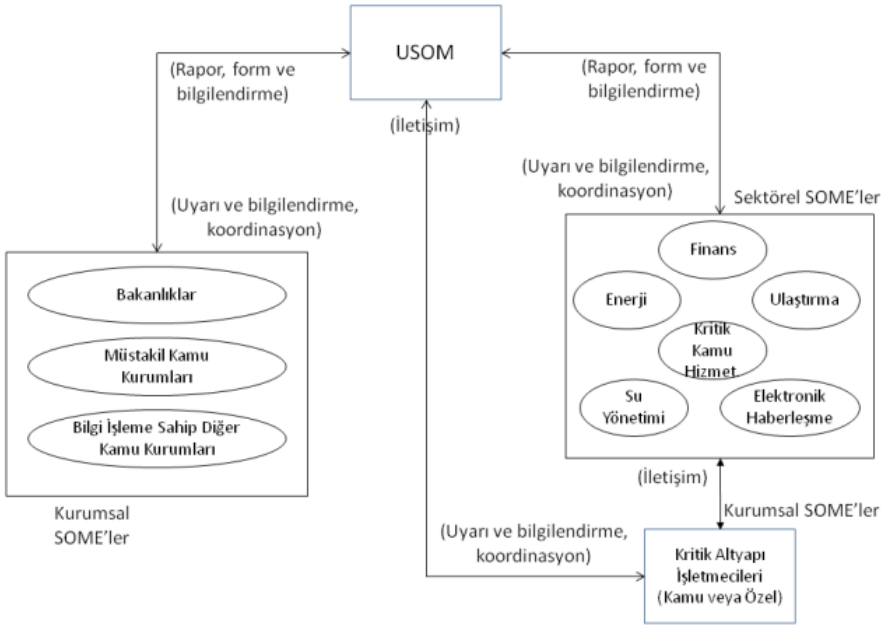
olaylarına maruz kalan bilişim sistemlerine yönelik koruyucu tedbirlerin alınması konusunda faaliyetlerde bulunur. Ayrıca yapılan siber güvenlik çalışmaları esnasında konusu suç teşkil eden bulgular ile karşılaşılması halinde adli makamlar ve kolluk kuvvetleri ile koordinasyon içerisinde hareket eder.

Bununla birlikte USOM tarafından hazırlanmış olan yerli ve milli SOME İletişim Portalı (SİP) üzerinden ülkemiz siber güvenlik organizasyonunda yer alan Sektörel ve Kurumsal SOME'lere güvenlik bildirimleri, alarm, duyuru, mesaj ve ihbarlar gönderilir. Aynı zamanda SOME'ler de SİP kanalı üzerinden tespit ettikleri ihbar ve olay bildirimlerini USOM'a iletebilmektedir. USOM'a gelen ihbar, olay bildirimlerin konusuna göre inceleme ve değerlendirmeler yapılarak gerekli aksiyonlar alınır veya aldırılır. USOM tarafından zararlı yazılım analizler çalışmaları yapılarak tespit edilen bulgular SOME'ler ve ilgili diğer paydaşlar ile paylaşılır. Zararlı internet adresleri olduğu tespit edilen oltalama, zararlı yazılım yayan ve/veya barından, komuta kontrol merkezi adresleri, port taraması yapan internet adreslerinin erişim engellemeleri yapılarak siber tehditlerin, olayların etkilerinin azaltılması, ortadan kaldırılması sağlanır. Bu faaliyetler siber tehditleri azaltmak, bertaraf etmek amaçlı 5809 sayılı elektronik haberleşme kanununda verilen yetki çerçevesinde yapılmaktadır.

Öte yandan USOM, ülkemizdeki kamu kurum ve kuruluşları, internet servis sağlayıcıları, özel sektör kuruluşları ve diğer internet aktörleri ile birlikte gerekli çalışmaları yapar. Siber güvenlik farkındalık faaliyetleri kapsamında Sektörel ve Kurumsal SOME'lere, üniversitelere, siber güvenlik topluluklarına yönelik olarak siber güvenlik eğitimi faaliyetlerinde bulunur. Ulusal ve uluslararası sivil, askeri siber güvenlik tatbikatlarına, NATO tatbikatlarına, konferanslara, çalıştaylara ve toplantılara katılım sağlar.

Kaynak: https://www.usom.gov.tr/hakkimizda

3. SOME (Siber Olaylara Müdahale Ekibi)



Şekil 1: Ulusal Siber Olaylara Müdahale Organizasyonu

Kaynaklar:
https://ibb.istanbul/ibb/bagli-kuruluslar-ve-istirakler/
https://www.usom.gov.tr/faydali-dokumanlar/kurumsal-some-rehberi
https://www.usom.gov.tr/faydali-dokumanlar/sektorel-some-rehberi

Ülkemizde Siber Güvenliğin sağlanması amacıyla kurulan USOM ve gerekli olan organizasyonu ifade eden "Kurumsal SOME Rehberi"'nde bulunan yukarıdaki şema nazara alındığı takdirde iş bu dosya konusu İBB (İstanbul Büyükşehir Belediyesi) bağlı kuruluşları ve iştirakleri değerlendirildiğinde Sektörel SOME 'ye dahil olan Ulaştırma, Su Yönetimi, Enerji ve Elektronik Haberleşme gibi sektörel bölüme ve dolayısıyla da Kurumsal SOME'lere bağlı organizasyon içerisinde olduğu anlaşılmaktadır.

4. "Dezenformasyon Yasası" olarak bilinen 7418 sayılı 'Basın Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun

Siber dünyanın bir başka alanı olan sosyal medya günümüzde etkin bir mecra olarak kabul edilmektedir. Tanınmış ya da popüler kişilerin milyonlarca kişi tarafından takip edildiği nazara alındığında bir siber güç olarak kullanılabileceği değerlendirilebilecektir. Bu güç ile sahte haber üretimi, manipüle edilmiş görsel ve videolar ve bilgiler yayılmasında rol alabilecektir. Bu nedenle yanlış bilginin yayılmasının önüne geçilmesi gerekmektedir. Dünyada farklı ülkelerde de bu ve benzeri kanunlar ile içeriklerin denetimi gerçekleştirilmektedir.

Kaynak:
https://www.resmigazete.gov.tr/eskiler/2022/10/20221018-1.htm
https://dbs.iletisim.gov.tr/

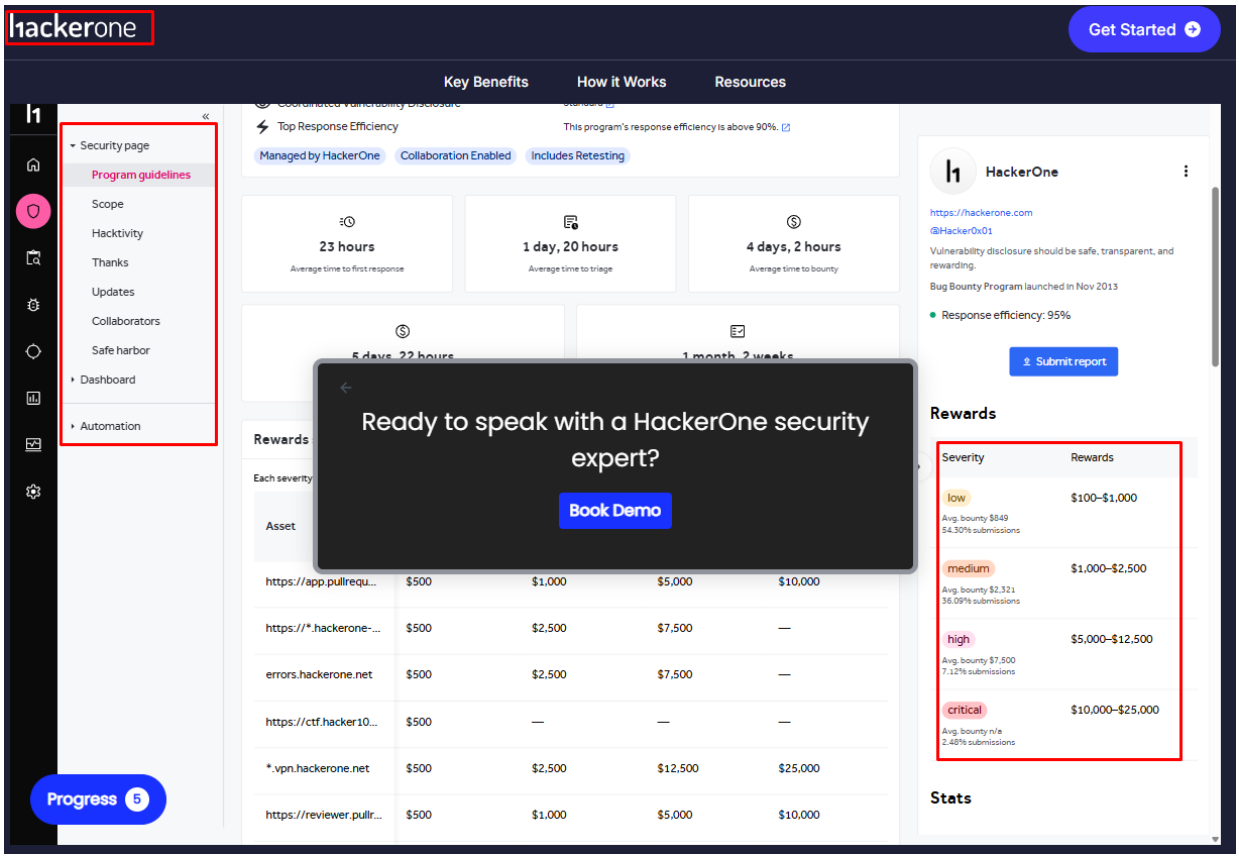
Kaynak: https://dbs.iletisim.gov.tr/hakikat/499

5. Sızma/Güvenlik Testleri

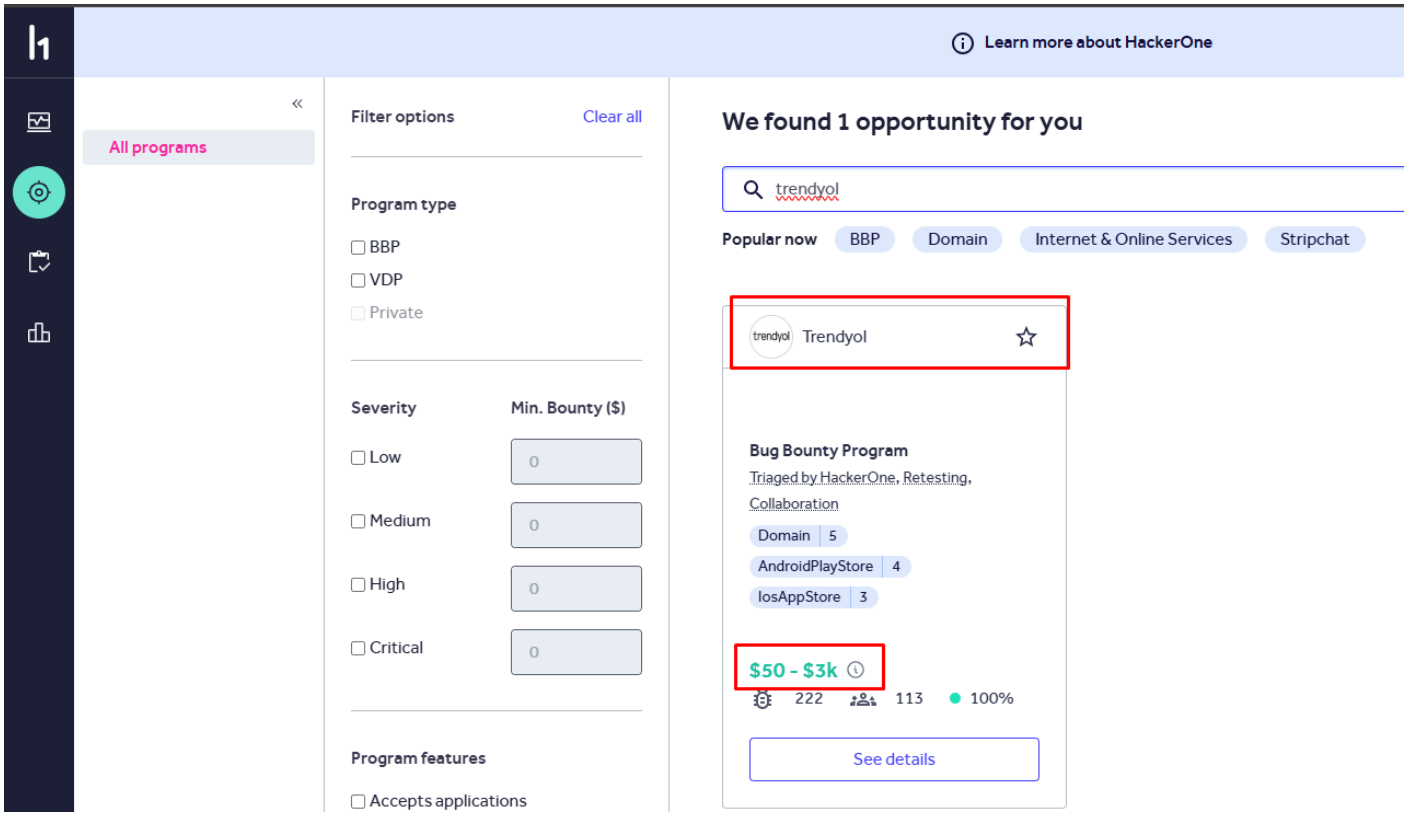
Sızma/Güvenlik testleri belirlenen sistemin veya ağın güvenlik açısından analiz edilmesi, sistemin güvenlik açıklarının ve güvenlik boşluklarının bulunması ile bu açıklardan faydalanılarak sistemlere sızılması işlemlerini kapsar. Web veya masaüstü yazılımlar özelinde de güvenlik açıklıkların analiz edilmesi ve bulunan açıklardan faydalanılarak yazılıma sızılması da güvenlik testleri olarak adlandırılabilir. Testler ulusal standardımız olan TS 13638 standardı kapsamında gerçekleştirilmektedir.

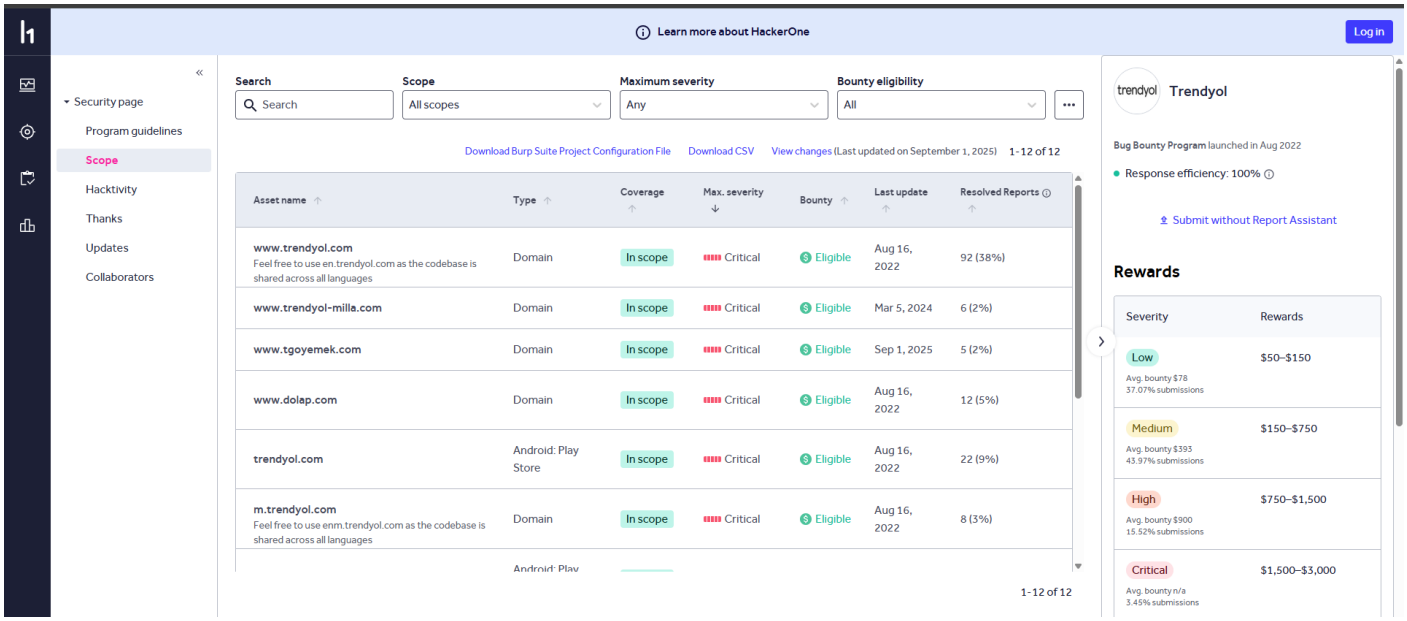
Kaynak:
https://www.tse.org.tr/sizma-testleri/

Sızma/Güvenlik testi çalışmaları bakış açısı olarak bir sisteme, sistemin sahibi tarafından yetkilendirilerek sistemlere zarar vermeden araştırmalarını ve sistemin açıklarının tespitinin yapılması için verilen bir hizmettir. Bu hizmetler ülkemizde ticari olarak yetkilendirilmiş şirketler tarafından verilmektedir. Üç sınıfa (A, B, C) ayrılmış olan yetki seviyeleri çerçevesinde bu hizmeti sağlamaktadırlar. Bunun yanında yetkin ve kabiliyetli kişilerden de şirketler hizmet almak istemektedirler. Bu kişilere şirketler veya kurumlar sistemlerindeki güvenlik açıklarını bulmaları için bağımsız araştırmacılara (etik hackerlara) ödül verdiği sistemlere BUG BOUNTY adı verilmektedir. Bu programları bir çatı altında toplayan ve hizmet verenlerden popüler olan şirketlerden biri de HackerOne platformudur. Bağımsız araştırmacılara belirlenmiş ve sınırlandırılmış bir kapsamda sistemlerin açıklarını bulmaları için desteklemekte, bulunan düşük, orta, yüksek ve kritik sistem açıklarına istinaden ödül (para) ödemektedirler.



İlgili platformda Dünyada tanınmış marka haline gelmiş birçok marka olduğu gibi ülkemizden Trendyol markası da bağımsız araştırmacıların bu hizmetinden faydalanmak için platformda olduğu bilinmektedir. Özetle sistemlerin güvenliklerinin sağlanması ve tehdit aktörleri (hacker) yasal alanlara yönlendirilerek bağımsız araştırmacı olmalarına destek olunduğu değerlendirilebilecektir.





E- TEHDİT AKTÖRLERİ VE HACKER PROFİLLERİ

Bir bilişim sistemine yetkisi olmadığı halde erişmeye çalışan, erişen, müdahale eden, erişmeyi engellemeye çalışan kişi/gruplara verilen tanımdır. Sektörde Beyaz (Etik) şapkalı ve Siyah şapkalı (Kişisel Kazanç/zarar verme) Hacker şeklinde temel iki gruba ayrılmaktadır. Bunlar dışında Gri Şapkalı Hacker, Hacktivist, Devlet Destekli Hacker ve Script Kiddie gibi farklı gruplara ayrılmış hacker türleri de bulunmaktadır.

Gerçek dünya gözlemlerine dayalı, küresel olarak erişilebilir bir düşman taktikleri ve teknikleri bilgi tabanı hazırlayan kuruluşlardan biri MITRE ATT&CK'dır. ATT&CK bilgi tabanı, özel sektörde, hükümette ve siber güvenlik ürün ve hizmet topluluğunda belirli tehdit modelleri ve metodolojilerinin geliştirilmesi için temel olarak kullanılmaktadır. ATT&CK tehdit aktörlerini sınıflandırarak bunları kategorize etmektedir.

Örneğin;

Star Blizzard : Star Blizzard, en az 2019'dan beri aktif olan, Rusya kökenli bir siber casusluk ve etki grubudur. Star Blizzard'ın kampanyaları Rus devletinin çıkarlarıyla yakından örtüşmekte olup, NATO ülkelerindeki, özellikle ABD ve İngiltere'deki akademik, savunma, hükümet, STK ve düşünce kuruluşlarına yönelik sürekli kimlik avı ve kimlik bilgilerinin çalınmasını içermektedir.

UNC3886: En az 2022'den beri aktif olan ve ABD ile Asya-Pasifik-Japonya (APJ) bölgelerinde bulunan savunma, teknoloji ve telekomünikasyon kuruluşlarını hedef alan Çin bağlantılı bir siber casusluk grubudur. UNC3886, sıfır gün güvenlik açıklarından yararlanarak ve yeni kötü amaçlı yazılım aileleri ve yardımcı programlar kullanarak uç cihazlar ve sanallaştırma teknolojileri konusunda derin bir anlayış sergilemiştir.

Transparent Tribe: En az 2013'ten beri aktif olan ve Pakistan merkezli olduğundan şüphelenilen bir tehdit grubudur. Başlıca hedef aldığı hedefler arasında Hindistan ve Afganistan'daki diplomatik, savunma ve araştırma kuruluşları yer almaktadır.

Kaynak:
https://attack.mitre.org/
https://attack.mitre.org/groups/G1033/
https://attack.mitre.org/groups/G1048/
https://attack.mitre.org/groups/G0134/

Hacker grupları tehdit grupları olarak ele alınmaktadır. Bu gruplar devlet destekli olabildiği gibi, istihbarat servislerine çalışan gruplar, aktivist grupları, itibar için çalışan gruplar, gelir/kazanç elde etmeye çalışan gruplar ya da bireyler olarak genel olarak sınıflandırılmaktadır.

F- VERİ SIZINTISI (DATA LEAK / DATA BREACH)

Tehdit grupları bir bilişim sistemine yetkisiz erişim sağladıklarında, bu sistemlerden veri çıkarma (data exfiltration) faaliyetinde bulunabilmektedir. Elde edilen verilerin yetkisiz şekilde ifşa edilmesi veya üçüncü taraflarla paylaşılması ise veri sızıntısı (data leak/breach) olarak tanımlanmaktadır.

Veri sızıntılarının kapsamı; erişilen sistemin niteliğine, faaliyet gösterilen sektöre ve tehdit aktörünün motivasyonuna bağlı olarak değişkenlik göstermektedir. Bu veriler arasında sistem bilgileri, ticari sırlar, sözleşmeler, finansal kayıtlar, stok verileri, çalışan bilgileri ve müşteri/üye verileri yer alabilmektedir.

Profesyonel/Uzman tehdit aktörlerinin genel yaklaşımı;

Profesyonel veya uzman seviyedeki tehdit aktörlerinin veri ihlali sonrası davranışları farklı motivasyonlara bağlı olarak değişebilmektedir.

Tehdit aktörlerinin temel motivasyonu itibar veya görünürlük sağlamak olduğunda, ele geçirilen veriler bazı durumlarda doğrudan internet ortamında, özellikle dark web forumları veya sızıntı platformları üzerinden yayımlanabilmektedir. Bu yaklaşım genellikle henüz tanınmışlık ve güvenilirlik kazanmamış, ekosistem içerisinde kendini konumlandırmaya çalışan kişi veya gruplarla ilişkilendirilmektedir.

Buna karşılık, siber suç ekosisteminde belirli bir tanınmışlık ve güven seviyesine ulaşmış tehdit grupları, ele geçirilen verileri çoğunlukla doğrudan kamuya açık ortamlarda paylaşmamaktadır. Bu aktörler verileri öncelikle kapalı iletişim ağlarında, iş birliği içerisinde oldukları kişi veya gruplarla paylaşarak finansal kazanç elde etmeyi hedefleyebilmektedir. Talep doğrultusunda ek veri toplama, hedefli veri çıkarma veya erişim devamlılığı sağlama gibi faaliyetler bu süreçte gözlemlenebilmektedir.

İlgili pazarlık ve ticari süreçlerin ardından veriler, "veri sızıntısı" veya "leak" başlığı altında dark web pazar yerleri ve forumlarda satışa sunulabilmektedir. Bu tür işlemlerde Bitcoin gibi kripto para birimleri yaygın olarak kullanılmaktadır. Satışa sunulan veriler; diğer tehdit aktörleri, dolandırıcılık grupları veya savunma amaçlı tehdit istihbaratı faaliyetleri yürüten kurum ve kuruluşlar tarafından edinilebilmektedir.

Son aşamada, finansal kazanç potansiyelinin azaldığı veya stratejik hedeflerin tamamlandığı durumlarda, tehdit aktörleri verileri itibar veya baskı oluşturma amacıyla kamuya açık şekilde yayımlayabilmektedir.

Veri ihlali izleme ve sızıntı indeksleme platformları, dijitalleşmenin artmasıyla birlikte veri ihlalleri (data breach) hem bireyler hem de kurumlar açısından önemli bir güvenlik riski haline gelmiştir. Bu kapsamda, internete ve dark web ortamlarına yansıyan sızıntı verilerini toplayan, indeksleyen ve sorgulanabilir hale getiren çeşitli platformlar ortaya çıkmıştır. Bu platformlar; kullanıcıların veya kurumların e-posta adreslerinin, kullanıcı adlarının ya da diğer kimlik bilgilerinin bilinen veri ihlallerinde yer alıp almadığını kontrol etmelerine imkân tanımaktadır.

Bu alanda öne çıkan platformlar arasında Have I Been Pwned (HIBP), DeHashed ve DataBreaches.net yer almaktadır. "Pwned" ifadesi hacker kültüründe "ele geçirilmiş" veya "kompromize edilmiş" anlamına gelir. HIBP bu terimi, bir kullanıcının bilgilerinin veri ihlali kapsamında ifşa edilmiş olmasını ifade etmek için kullanır.

G- DARKNET VE DARK WEB KAVRAMLARI

İnternetin, herkes tarafından doğrudan erişilemeyen ve özel yazılım veya yapılandırmalar gerektiren bölümleri bulunmaktadır. Bu kavramlar sıklıkla birbirine karıştırılsa da aynı anlama gelmez.

Dark Web, bu ortamda yer alan içerik ve verileri ifade ederken; Darknet, bu içeriklerin barındırıldığı ağ altyapısını tanımlamaktadır.

Herkese açık internet kaynaklarına standart tarayıcılar aracılığıyla erişilebilirken, darknet ve dark web ortamlarına erişim özel araçlar gerektirmektedir. Tanım teknik olarak bu şekilde yapılmakla birlikte, kavramların daha kolay anlaşılabilmesi için aşağıdaki gibi sadeleştirilebilir.

Çeşitli ülkelerde sosyal medya platformlarına yönelik bant genişliği daraltma veya erişim kısıtlama uygulamaları görülebilmektedir. Bu tür kısıtlamalar karşısında kullanıcılar VPN gibi anonimleştirme ve yönlendirme teknolojilerine başvurabilmektedir. Benzer biçimde, geleneksel internet altyapısında yer almayan darknet ve dark web ortamlarına erişim de TOR gibi özel yazılımlar (tarayıcı) aracılığıyla sağlanabilmektedir. TOR, bu amaçla kullanılan en yaygın anonim iletişim araçlarından biridir.

Tor Project, Inc., 2006 yılında 501(c)(3) kâr amacı gütmeyen bir kuruluş haline geldi, ancak "soğan yönlendirme" fikri 1990'ların ortalarında ortaya çıktı.

Tor kullanıcıları gibi, Tor'u mümkün kılan geliştiriciler, araştırmacılar ve kurucular da çeşitli bir grup insandan oluşuyor. Ancak Tor'da yer alan tüm bu insanları birleştiren ortak bir inanç var: İnternet kullanıcıları sansürsüz bir web'e özel erişime sahip olmalıdır.

1990'larda internetin güvenlik açığı ve izleme ve gözetleme amacıyla kullanılabilme özelliği giderek belirginleşiyordu ve 1995'te ABD Deniz Kuvvetleri Araştırma Laboratuvarı'nda (NRL) David Goldschlag, Mike Reed ve Paul Syverson, kimin kiminle konuştuğunu, hatta ağı izleyen birine bile belli etmeyen internet bağlantıları oluşturmanın bir yolu olup olmadığını sorguladılar. Cevapları, soğan yönlendirmesinin ilk araştırma tasarımlarını ve prototiplerini oluşturmak ve uygulamaya koymak oldu.

Tor Projesi olarak, herkesin sansürsüz bir internete özel erişime sahip olması için her gün mücadele ediyoruz ve Tor, çevrimiçi gizlilik ve özgürlük için dünyanın en güçlü aracı haline geldi.

Ancak Tor, sadece bir yazılımdan ibaret değil. İnsan haklarına adanmış uluslararası bir topluluğun sevgiyle ürettiği bir proje. Tor Projesi, şeffaflığa ve kullanıcılarının güvenliğine derinden bağlıdır.

Kaynak: https://www.torproject.org/about/history/

TOR ağında kullanılan "soğan yönlendirme" (Onion Routing) kavramı, İngilizce'de "soğan" anlamına gelen onion kelimesinden türetilmiştir. Bu yapı, kullanıcı trafiğinin çok katmanlı şifreleme ile anonimleştirilmesini ifade eder.

TOR ağına erişim sağlandığında geleneksel internet alan adları (.com, .gov, .edu vb.) tamamen ortadan kalkmaz; ancak TOR'a özgü gizli servisler ".onion" uzantısı ile adreslenir. Bu uzantılar yalnızca TOR ağı üzerinden erişilebilen servisleri temsil eder.

Örneğin, kamuya açık bir alan adı olan uyap.gov.tr, TOR ağına geçildiğinde otomatik olarak uyap.onion şeklinde dönüşmez. TOR üzerindeki servisler, ayrı yapılandırılan ve genellikle rastgele üretilmiş .onion adreslerine sahiptir. Güvenlik ve anonimlik gereksinimleri nedeniyle bu adresler çoğunlukla kurumsal alan adlarıyla birebir eşleşmez.

uyap.gov.tr adresi aşağıdaki gibi anlaşılmaz bir hal alacaktır.

http://6nhmgdpnyoljhzr5kwlatx2u3diou4ldeofxjz3wkhalzgjqxzqd.onion/

Herkese açık internet ortamında, örneğin Google üzerinden arama yapılabildiği gibi, TOR ağı gibi ağlar üzerinde barındırılan içeriklere erişmek için TORCH veya DuckDuckGo gibi arama servisleri kullanılabilmektedir.

Darknet, geleneksel internetten tamamen ayrı bir ağ değil; özel protokoller ve yazılımlar aracılığıyla erişilebilen alternatif bir iletişim katmanıdır. TOR gibi anonimlik odaklı yazılımlar sayesinde darknet üzerinde yer alan dark web içeriklerine erişim sağlanabilir.

Özetle DARKNET/DARKWEB kapalı kaynak değil, herkes tarafından erişilebilen ancak bilgi/tecrübe sahibi olunması gereken açık kaynak erişimlerin olduğu bir alandır.

H- DARK WEB İÇERİK EKOSİSTEMİ

Dark Web içerik ekosistemi, özel yazılımlar ve anonimleştirme teknolojileri kullanılarak erişilebilen ağ ortamlarında faaliyet gösteren platformlar, kullanıcılar ve dijital hizmetlerden oluşan yapıyı ifade etmektedir. Bu ekosistem genellikle Tor ağı üzerinde barındırılan ".onion" uzantılı servisler aracılığıyla erişilebilir durumdadır.

Dark Web, teknik olarak bir altyapıdan ziyade içerik ve hizmet katmanını ifade ederken; bu içeriklerin barındırıldığı anonim ağ yapısı "darknet" olarak tanımlanmaktadır. Ekosistem; forumlar, pazar yerleri, veri paylaşım platformları, iletişim servisleri ve yasa dışı hizmet sağlayıcılarından oluşmaktadır.

Dark web forumları, tehdit aktörlerinin iletişim kurduğu, bilgi paylaştığı ve iş birliği yaptığı platformlardır.

Bu forumlarda:
- Sızdırılmış veri duyuruları
- Yeni zararlı yazılım tanıtımları
- Güvenlik açığı satış ilanları
- "Initial Access" (ilk erişim) satışları
- Dolandırıcılık yöntemleri gibi içerikler paylaşılabilmektedir.

Örneğin bir tehdit aktörü, ele geçirdiği bir kuruma ait veriyi forumda duyurarak hem itibar kazanmayı hem de alıcı bulmayı hedefleyebilir.

I- Siber Tehdit İstihbaratı (Cyber Threat Intelligence – CTI)

Dijital/Sanal/Siber/Siber Uzay ortamında savunma sağlayabilmek için tehdit aktörleri ve tehditler hakkında bilgi toplama, analiz etme ve savunma stratejileri geliştirme amaçlı olarak yapılan çalışmalardır. Genel olarak geleneksel istihbarat çalışmalarının birçok farklı şekilde ifade edilen Dijital/Sanal/Siber/Siber Uzay ortamında gerçekleştirilen faaliyetleridir.

Yakın tarihte (19/09/2025) İngiliz gizli servisi İstanbul Konsolosluğunda siber casusluk için yeni uygulaması olan "Sessiz Kurye" yazılımını tanıttı. Ülkeler artık istihbarat ve savaş ortamını dijital dünyaya yani Siber Uzaya taşımaktadır. Bu kavramlara da Siber İstihbarat ve Siber Savaş denilmektedir.

İngiliz gizli servisinden muhbir hattı… MI6 'Sessiz Kurye'yi İstanbul'da tanıttı.

Kaynak:
https://www.ntv.com.tr/dunya/ingiltereden-casuslara-ozel-mesajlasma-uygulamasi-bugun-istanbulda-tanitilacak,eaclYzP6vk-ephIPmrlpXw
https://www.sozcu.com.tr/istanbul-da-bugun-ingilizler-gizli-uygulamasini-tanitacak-p229107
https://www.hurriyet.com.tr/dunya/ingiliz-gizli-servisinden-muhbir-hatti-mi6-sessiz-kuryeyi-istanbulda-tanitti-42954943
https://www.bbc.com/turkce/articles/c9wdy1jk9x9o

İ- OSINT * AÇIK KAYNAK İSTİHBARATI (OPEN SOURCE INTELLİGENCE – OSINT)

Herkese açık ve yasal yollarla erişilebilen kaynaklardan elde edilen verilerin sistematik biçimde toplanması, doğrulanması, analiz edilmesi ve anlamlı istihbarata dönüştürülmesi sürecidir. Bu konuda birçok açık kaynak bulunduğu gibi birçok kitapta yazılmıştır.

OSINT 101 Handbook: Advanced Reconnaissance, Threat Assessment, And Counterintelligence
ISBN-10 : 1839385464

OSINT Techniques: Resources for Uncovering Online Information
ISBN-13 : 979-8345969250

Deep Dive: Exploring the Real-World Value of Open Source Intelligence
ISBN-13 : 978-1119933243

Grey Area: Dark Web Data Collection and the Future of Osint
ISBN-13 : 978-1394357277

Operator Handbook: Red Team + OSINT + Blue Team Reference
ISBN-13 : 979-8605493952

OSINT, kamuya açık internet kaynakları, medya içerikleri, akademik yayınlar, resmî veritabanları, sosyal medya platformları, ticari veri sağlayıcıları, forumlar ve topluluklar gibi açık kaynaklardan elde edilen verilerin istihbarata dönüştürülmesini ifade eder.

Veriler; devlet kurumları, askerî yapılar, kolluk kuvvetleri, kurumsal şirketler, siber güvenlik ekipleri, gazeteciler ve akademisyenler tarafından kullanılmaktadır.

OSINT çalışmaları genellikle klasik istihbarat döngüsünü takip eder:

Planlama – Hedef ve kapsam belirleme
Toplama – Açık kaynaklardan veri toplama
Doğrulama – Kaynak güvenilirliğini kontrol etme
Analiz – Veriyi anlamlandırma
Raporlama – Karar vericiye sunma

J- YAYGIN KİMLİK DOĞRULAMA ALIŞKANLIKLARI VE PAROLA GÜVENLİĞİ

Genel olarak kurum ve şirketlerde çalışanların kullanıcı adları belirli bir strateji doğrultusunda verilmektedir. Bilgisayar kullanıcı adı ile e-posta adresleri farklı olabildiği gibi aynı olarak da kullanılabilmektedir.
Yüksek öneme sahip kamu kurumlarında çalışan sayısı yüksek olduğundan isim ve soyisim kullanımı aynı isim soy isme sahip personel olabileceğinden bilgisayar açılışında kullanıcı adı olarak sicil numaraları kullanılabilmektedir**.** Şirketlerde ise bu durum isim.soyisim, ismin başharfi soyisim gibi farklı şekillerde kullanılabilmektedir. Özetle kullanıcı adı belirleme kuralları ve şablonları bulunmaktadır. Örneğin çalışanın isim ve soy isminin Ahmet Yılmaz olduğu varsayıldığında aşağıdaki gibi örnekler kullanıcı adı olarak kullanılabilecektir. Amaç standart bir kullanıcı adı politikası kullanmaktır.

Ahmetyilmaz
Ahmet.yilmaz
Ayilmaz

Ahmety
Ayilmaz1
Ahmety

1- Parola/ Kimlik Doğrulama Politikaları

Aynı şekilde parola kullanımında da belirli bir politika olması gerekmektedir. Ancak bu politika belirlenirken siber güvenlik trendleri takip edilerek güvenli parolalar kullanılması gerekmektedir.

Günümüzde parola politikaları karmaşık parola kullanımına yönlendirmektedir. Karmaşık parolalar en az 8 karakter olması, en az bir büyük ve küçük harf içermesi, özel karakter kullanılması (*/./!/+ vb.) gibi standartlar belirlenmektedir. Daha güçlü parola kullanımında ise sınırlamalar doğum yılının kullanılmaması, şirket isminin, kullanıcının adı ve soyadını içermemesi gibi kurallar da belirlenebilmektedir. Bunun yanı sıra güvenliği arttırmak adına birden fazla parola yada aşama kullanılarak MFA (Multi Factor Authentication – Çok Faktörlü Kimlik Doğrulama) doğrulama yapılması ya da 2FA (Two Factor Authentication – iki faktörlü kimlik doğrulama) ile kimlik doğrulaması yapılması da mümkündür. 2FA kullanımı yapılırken OTP (One Time Password – Tek Seferlik Parola) da kullanılabilmektedir.

Bunların en yaygın örneği ise bankaların kullandığı ilk girişte müşteri no/tc kimlik no ile bir parola girişi yaptırılması, ardından bir fotoğraf gösterilmesi, sonrasında ise SMS (Small Message Service – Kısa Mesaj Servisi) ile gelen parolanın girişinin yaptırılması gibi çoklu kimlik doğrulama yöntemlerinin kullanılması güvenlik için gereklidir.

2- Yazılımlarda Merkezi Kullanıcı Adı ve Parola Politikaları

Kurum ve şirketler, kullanıcı kimlik doğrulama ve yetkilendirme süreçlerini güvenli ve merkezi bir yapı üzerinden yönetmektedir. Bu kapsamda en yaygın kullanılan çözümlerden biri Microsoft tarafından geliştirilen Active Directory dizin hizmetidir. Active Directory; kimlik doğrulama (authentication), yetkilendirme (authorization) ve güvenlik politikalarının merkezi olarak uygulanmasını sağlamaktadır.

Kurumlar, iş süreçlerine bağlı olarak üçüncü taraf yazılımlar kullanabildikleri gibi, kendi yazılım geliştirme ekipleri aracılığıyla özel uygulamalar da geliştirebilmektedir. Bu uygulamaların da kullanıcı kimlik doğrulama mekanizmasına ihtiyacı bulunmaktadır.

Yazılım geliştirme sürecinde kimlik yönetimi iki farklı yöntemle sağlanabilmektedir: Merkezi dizin hizmeti (örneğin Active Directory) ile entegrasyon sağlamak veya uygulamaya özgü bir kimlik doğrulama altyapısı oluşturmak. Merkezi entegrasyon yaklaşımı, kullanıcıların tek bir kimlik ile birden fazla sisteme erişebilmesini sağlayan Single Sign-On (SSO) ve federated identity modellerine imkân tanımaktadır.

Türkiye'de kullanılan e-Nabız sistemi bu duruma örnek olarak gösterilebilir. Kullanıcılar sisteme doğrudan kendi oluşturdukları kimlik bilgileriyle giriş yapabildikleri gibi, e-Devlet kimlik doğrulama altyapısı üzerinden de erişim sağlayabilmektedir. Bu yapı, farklı kimlik doğrulama mekanizmalarının entegre çalışabildiğini ve federasyon modelinin uygulandığını göstermektedir.

BİLİRKİŞİ RAPORU
BÖLÜM – 2
TEKNİK ANALİZ

Görevlendirme kapsamında sanık Hüseyin GÜN'ün 26/10/2025 tarihli kolluk ifadesinin 123., 124. Ve 125. Sayfalarında yer alan ekran görüntülerinin analizi ve açıklanması istenmiştir.

Öncelikle inceleme yapılmadan önce verilerin anlamlandırılması için temizlenmesi gerekmektedir. Temizleme işlemi tekrar eden kayıtların, eşleştirilebilen kayıtların, anlamlı kayıtların bir araya getirilmesi anlamına gelmektedir.

123. sayfa ***İBB.GOV.TR yazılı olmasına karşın devamında bir bilgi bulunmamaktadır. 124. Sayfadan anlaşıldığı üzere sayfaya ilgili ekran alıntısı sığmadığı için dosya kapsamında incelemeye ilişkin veri olmadığından iş bu raporda 123.sayfayla ilgili bir değerlendirme yapılmamaktadır.

124.Sayfa 'da bir adet ekran görüntüsünde bulunan ibb.gov.tr uzantılı e-posta adresleri aşağıdaki gibidir.

124. Sayfa Ekran Alıntısı			
Kullanıcı Adı/E-posta	**Parola**	**_index**	**_type**
isfalt@ibb.gov.tr	886777	leak-jan19_20190314	leakDoc
h.karakaya@ibb.gov.tr	Kiraz44	leak-jan19_20190314	leakDoc
mcavus@ibb.gov.tr	54492	leak-jan19_20190314	leakDoc
h.gencdal@ibb.gov.tr	1938	leak-jan19_20190314	leakDoc
f.yilmaz@ibb.gov.tr	31996	leak-jan19_20190314	leakDoc
h.zeyveli@ibb.gov.tr	61990	leak-jan19_20190314	leakDoc
nefise.uygun@ibb.gov.tr	milzzy23su26iplnum	leak-jan19_20190314	leakDoc
naile.sen@ibb.gov.tr	nayle16	leak-jan19_20190314	leakDoc
nefise.uygun@ibb.gov.tr	alchock	leak-jan19_20190314	leakDoc

125.Sayfa 'da bulunan **birinci ekran görüntüsü** ibb.gov.tr uzantılı e-posta adresleri aşağıdaki gibidir.

125. Sayfa 1. Ekran Alıntısı			
Kullanıcı Adı/E-posta	**Parola**	**_index**	**_type**
saliha.peru@ibb.gov.tr	MjAxMTY4	leak-jan19_20190314	leakDoc
hsan@ibb.gov.tr	123654	leak-jan19_20190314	leakDoc
beyazmasa@ibb.gov.tr	tural1	leak-jan19_20190314	leakDoc
bozkul@ibb.gov.tr	362514	leak-jan19_20190314	leakDoc
alpergo@ibb.gov.tr	83953	leak-jan19_20190314	leakDoc
isfalt@ibb.gov.tr	JCYRVP	leak-jan19_20190314	leakDoc
burhanayan@ibb.gov.tr	1119734	leak-jan19_20190314	leakDoc

ikizzeynep.mutlu@ibb.gov.tr	semih1972	leak-jan19_20190314	leakDoc
adilyildirim@ibb.gov.tr	484b43	leak-jan19_20190314	leakDoc

125.Sayfa 'da bulunan **ikinci ekran görüntüsü** ibb.gov.tr uzantılı e-posta adresleri aşağıdaki gibidir.

125. Sayfa 2. Ekran Alıntısı			
Kullanıcı Adı/E-posta	**Parola**	**_index**	**_type**
ibasaran@ibb.gov.tr	2550as	leak-myspace-20170910	myspace
bilinmiyor **(isfalt@ibb.gov.tr)**	886777	leak-jan19_20190314	leakDoc
bilinmiyor **(h.karakaya@ibb.gov.tr)**	Kiraz44	leak-jan19_20190314	leakDoc
bilinmiyor **(mcavus@ibb.gov.tr)**	52492	leak-jan19_20190314	leakDoc
bilinmiyor **(h.gencdal@ibb.gov.tr)**	1938	leak-jan19_20190314	leakDoc
bilinmiyor **(f.yilmaz@ibb.gov.tr)**	31996	leak-jan19_20190314	leakDoc

125. Sayfa 'da bulunan ikinci ekran görüntüsünde farklı olarak değerlendirilen tek kayıt ibasaran@ibb.gov.tr olduğu değerlendirilmektedir. Kullanıcı adı/E-posta, Parola, _index ve _type verileri farklılık göstermektedir.

125. Sayfa 'da bulunan **ikinci ekran görüntüsündeki** diğer tüm kayıtların kullanıcı adı / eposta bölümleri görünmediğinden dolayı "**bilinmiyor**" olarak değerlendirilmiştir. Sonrasında ise parolalar nazara alındığında 124. Sayfadaki kullanıcı adı/eposta bölümündeki kullanıcıların parolaları ile aynı olduğu, _index ve _type bölümündeki değerlerinde aynı olduğu tespit edilmiştir. Buna ilişkin ekran görüntüleri incelendiğinde 124. sayfada sadece verilerin olduğu, 125. sayfada bulunan ikinci ekran görüntüsünde ise kullanılan yazılımın ekran görüntüsünün de görünür şekilde olması sebebiyle ilgili kayıtların 124. Sayfadaki kayıtlarla eşleştiği değerlendirilmektedir. Tekil veri olduğu değerlendirilen _id bölümündeki verilerinde eşleştiği tespit edildiğinden ilgili kayıtların aynı kayıtlar olduğu tespit edilmiştir. Mükerrer veriler tablodan çıkarılmıştır.

124. Sayfa Ekran Alıntısı			
Kullanıcı Adı/E-posta	**Parola**	**_index**	**_type**
isfalt@ibb.gov.tr	886777	leak-jan19_20190314	leakDoc
h.karakaya@ibb.gov.tr	Kiraz44	leak-jan19_20190314	leakDoc
mcavus@ibb.gov.tr	54492	leak-jan19_20190314	leakDoc
h.gencdal@ibb.gov.tr	1938	leak-jan19_20190314	leakDoc
f.yilmaz@ibb.gov.tr	31996	leak-jan19_20190314	leakDoc
h.zeyveli@ibb.gov.tr	61990	leak-jan19_20190314	leakDoc
nefise.uygun@ibb.gov.tr	milzzy23su26iplnum	leak-jan19_20190314	leakDoc
naile.sen@ibb.gov.tr	nayle16	leak-jan19_20190314	leakDoc
nefise.uygun@ibb.gov.tr	akchock	leak-jan19_20190314	leakDoc
125. Sayfa 1. Ekran Alıntısı			
Kullanıcı Adı/E-posta	**Parola**	**_index**	**_type**
saliha.peru@ibb.gov.tr	MjAxMTY4	leak-jan19_20190314	leakDoc
hsan@ibb.gov.tr	123654	leak-jan19_20190314	leakDoc
beyazmasa@ibb.gov.tr	tural1	leak-jan19_20190314	leakDoc

bozkul@ibb.gov.tr	362514	leak-jan19_20190314	leakDoc
alpergo@ibb.gov.tr	83953	leak-jan19_20190314	leakDoc
isfalt@ibb.gov.tr	JCYRVP	leak-jan19_20190314	leakDoc
burhanayan@ibb.gov.tr	1119734	leak-jan19_20190314	leakDoc
ikizzeynep.mutlu@ibb.gov.tr	semih1972	leak-jan19_20190314	leakDoc
adilyildirim@ibb.gov.tr	484b43	leak-jan19_20190314	leakDoc

125. Sayfa 2. Ekran Alıntısı			
Kullanıcı Adı/E-posta	**Parola**	**_index**	**_type**
ibasaran@ibb.gov.tr	2550as	leak-myspace-20170910	myspace

Temizlenmiş veriler değerlendirildiğinde iş bu raporun birinci bölümünün **J- YAYGIN KİMLİK DOĞRULAMA ALIŞKANLIKLARI VE PAROLA GÜVENLİĞİ** maddesinde ifade edilen yaygınlaşmış kullanıcı adı politikasına uygun kullanıcı adları olduğu değerlendirilebilecektir.

Temizlenmiş veriler değerlendirildiğinde raporun birinci bölümünün **J- YAYGIN KİMLİK DOĞRULAMA ALIŞKANLIKLARI VE PAROLA GÜVENLİĞİ** maddesinde ifade edilen yaygınlaşmış parola politikasına **uygun olmadığı değerlendirilmektedir**. En kısa parola sadece rakamlardan oluşan ve dört karakter uzunluğunda olduğu tespit edilmektedir. Sadece harflerden oluşan parolalar olduğu gibi karmaşık olarak ifade edilebilecek sadece özel karakter bulunmayan parolaların da olduğu anlaşılmaktadır.

isfalt@ibb.gov.tr ve nefise.uygun@ibb.gov.tr kullanıcı/e-posta adresleri farklı şifrelere sahip olması birden fazla veri sızıntısında farklı şifrelerle olduğu değerlendirildiğinden mükerrer olan isfalt@ibb.gov.tr ve nefise.uygun@ibb.gov.tr adresleri tekilleştirilmiştir. Tüm kullanıcılar tekilleştirildikten sonra toplam 17 adet kullanıcı/e-posta adresi olduğu tespit edilmektedir. Kullanıcıların hangi sızıntıda ortaya çıktığı araştırılacağından parola kısımları da ihtiyaç duyulmayacağından temizlenmiş veri aşağıdaki tabloda görülmektedir.

124. Sayfa Ekran Alıntısı (8 Kullanıcı)		
Kullanıcı Adı	**_index**	**_type**
isfalt@ibb.gov.tr	leak-jan19_20190314	leakDoc
h.karakaya@ibb.gov.tr	leak-jan19_20190314	leakDoc
mcavus@ibb.gov.tr	leak-jan19_20190314	leakDoc
h.gencdal@ibb.gov.tr	leak-jan19_20190314	leakDoc
f.yilmaz@ibb.gov.tr	leak-jan19_20190314	leakDoc
h.zeyveli@ibb.gov.tr	leak-jan19_20190314	leakDoc
nefise.uygun@ibb.gov.tr	leak-jan19_20190314	leakDoc
naile.sen@ibb.gov.tr	leak-jan19_20190314	leakDoc
125. Sayfa 1. Ekran Alıntısı (8 Kullanıcı)		
Kullanıcı Adı	**_index**	**_type**
saliha.peru@ibb.gov.tr	leak-jan19_20190314	leakDoc
hsan@ibb.gov.tr	leak-jan19_20190314	leakDoc
beyazmasa@ibb.gov.tr	leak-jan19_20190314	leakDoc

bozkul@ibb.gov.tr	leak-jan19_20190314	leakDoc
alpergo@ibb.gov.tr	leak-jan19_20190314	leakDoc
burhanayan@ibb.gov.tr	leak-jan19_20190314	leakDoc
ikizzeynep.mutlu@ibb.gov.tr	leak-jan19_20190314	leakDoc
adilyildirim@ibb.gov.tr	leak-jan19_20190314	leakDoc
125. Sayfa 2. Ekran Alıntısı (1 Kullanıcı)		
Kullanıcı Adı	**_index**	**_type**
ibasaran@ibb.gov.tr	leak-myspace-20170910	myspace

125. Sayfa 'da bulunan **ikinci ekran görüntüsündeki** 1,259,210 hits olarak görünen bilginin doğruluğu değerlendirilemeyecektir. Ekran görüntüsünde bir yazılım olduğu değerlendirildiğinde yazılım içerisindeki verilerde "@ibb.gov.tr" ifadesi geçen verilerin sorgulandığı anlaşılmaktadır. Ancak sonuçlarda bulunan yani "hits" olarak ifade edilecek ekran görüntüsünde sarı olarak işaretli kayıtların bazıları "ibb.gov.tr" bazıları ise "gov.tr" olarak sarı işaretli olduğu görülmektedir. Aynı şekilde bir kayıt olarak ifade edilmesi gerekli olmasına rağmen aynı kayıt içerisinde geçen iki adet ibb.gov.tr adresini de mükerrer saymış olabileceği değerlendirilmektedir. İzah edilen nedenlerden dolayı 1,259,210 hits olarak görünen bilginin güvenilir ve doğru olmadığı değerlendirilmektedir.

17 adet kullanıcı/eposta adresi bilinen üç farklı platformda sorgulandığı takdirde aşağıdaki detayda sonuçlar elde edilmiştir.

Sızıntı Tespiti **(https://app.dehashed.com/)**

No	Kullanıcı/Eposta	Sızıntı Adedi	Sızıntı Tanımı
1	isfalt@ibb.gov.tr	1	Collections
2	h.karakaya@ibb.gov.tr	1	Collections
3	mcavus@ibb.gov.tr	1	Collections
4	h.gencdal@ibb.gov.tr	1	Collections
5	f.yilmaz@ibb.gov.tr	1	Collections
6	h.zeyveli@ibb.gov.tr	1	Collections
7	nefise.uygun@ibb.gov.tr	4	Exploit.in Exploit.in Collections AntiPublic
8	naile.sen@ibb.gov.tr	1	AntiPublic
9	saliha.peru@ibb.gov.tr	3	MyHeritage.com Twitter.com Dailymotion
10	hsan@ibb.gov.tr	2	Collections Collections
11	beyazmasa@ibb.gov.tr	0	Bilgi bulunmamaktadır.
12	bozkul@ibb.gov.tr	0	Bilgi bulunmamaktadır.
13	alpergo@ibb.gov.tr	0	Bilgi bulunmamaktadır.

14	burhanayan@ibb.gov.tr	0	Bilgi bulunmamaktadır.
15	ikizzeynep.mutlu@ibb.gov.tr	0	Bilgi bulunmamaktadır.
16	adilyildirim@ibb.gov.tr	0	Bilgi bulunmamaktadır.
17	ibasaran@ibb.gov.tr	2	AntiPublic Myspace.com

Sızıntı Tespiti **(https://databreach.com/)**

No	Kullanıcı/Eposta	Sızıntı Adedi	Sızıntı Tarihi	Sızıntı Tanımı
1	isfalt@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
2	h.karakaya@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
3	mcavus@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
4	h.gencdal@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
5	f.yilmaz@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
6	h.zeyveli@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
7	nefise.uygun@ibb.gov.tr	4	7 Ocak 2019 16 Aralık 2016 13 Ekim 2016 1 Ocak 2014	Collection #1-5 Anti Public Exploit.in Ubisoft Forum
8	naile.sen@ibb.gov.tr	3	7 Ocak 2019 16 Aralık 2016 13 Ekim 2016	Collection #1-5 Anti Public Exploit.in
9	saliha.peru@ibb.gov.tr	5	2 Nisan 2025 1 Ocak 2021 7 Ocak 2019 26 Ekim 2017 20 Ekim 2016	X (Twitter) Twitter Collection #1-5 MyHeritage Dailymotion
10	hsan@ibb.gov.tr	2	4 Kasım 2020 7 Ocak 2019	Cit0day Collection #1-5
11	beyazmasa@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
12	bozkul@ibb.gov.tr	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5
13	alpergo@ibb.gov.tr	1	7 Ocak 2019	Collection#1-5
14	burhanayan@ibb.gov.tr	1	7 Ocak 2019	Collection#1-5

15	ikizzeynep.mutlu@ibb.gov.tr	1	7 Ocak 2019	Collection#1-5
16	adilyildirim@ibb.gov.tr	1	7 Ocak 2019	Collection#1-5
17	ibasaran@ibb.gov.tr	4	7 Ocak 2019 16 Aralık 2016 13 Ekim 2016 1 Temmuz 2008	Collection#1-5 Anti Public Exploit.in MySpace

1- isfalt@ibb.gov.tr – 4 adet Sızıntı - HIBP (haveibeenpwned.com)

Sızıntı Tarihi	Sızıntı Tanımı	Sızan Veri Tipi	Sızıntı Açıklaması EN	Sızıntı Açıklaması TÜRKÇE (Google Translate)
Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.

Ekim 2019	Data Enrichment Exposure From PDL Customer	Email addresses Employers Geographic locations Job titles Names Phone numbers Social media profiles	In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.	Ekim 2019'da güvenlik araştırmacıları Vinny Troia ve Bob Diachenko, 1,2 milyar kişisel veri kaydı içeren korumasız bir Elasticsearch sunucusu tespit etti. Açığa çıkan veriler arasında, veri zenginleştirme şirketi People Data Labs'ten (PDL) kaynaklandığını gösteren bir indeks ve 622 milyon benzersiz e-posta adresi bulunuyordu. Sunucu PDL'ye ait değildi ve bir müşterinin veritabanını düzgün bir şekilde güvence altına almadığı düşünülüyor. Açığa çıkan bilgiler arasında e-posta adresleri, telefon numaraları, sosyal medya profilleri ve iş geçmişi verileri yer alıyordu.
Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu.

			addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.
Ocak 2017	River City Media Spam List	Email addresses IP addresses Names Physical addresses	In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.	Ocak 2017'de, River City Media'ya ait devasa bir veri yığını internette ifşa edildi. Verilerde, e-posta ve IP adresleri, isimler ve fiziksel adresler de dahil olmak üzere yaklaşık 1,4 milyar kayıt bulunduğu ve bunların tamamının devasa bir spam operasyonunun parçası olarak kullanıldığı tespit edildi. Yinelenen kayıtlar ayıklandıktan sonra, ifşa edilen verilerde 393 milyon benzersiz e-posta adresi olduğu ortaya çıktı.

2- h.karakaya@ibb.gov.tr – 5 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.

Ekim 2019	Data Enrichment Exposure From PDL Customer	Email addresses Employers Geographic locations Job titles Names Phone numbers Social media profiles	In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.	Ekim 2019'da güvenlik araştırmacıları Vinny Troia ve Bob Diachenko, 1,2 milyar kişisel veri kaydı içeren korumasız bir Elasticsearch sunucusu tespit etti. Açığa çıkan veriler arasında, veri zenginleştirme şirketi People Data Labs'ten (PDL) kaynaklandığını gösteren bir indeks ve 622 milyon benzersiz e-posta adresi bulunuyordu. Sunucu PDL'ye ait değildi ve bir müşterinin veritabanını düzgün bir şekilde güvence altına almadığı düşünülüyor. Açığa çıkan bilgiler arasında e-posta adresleri, telefon numaraları, sosyal medya profilleri ve iş geçmişi verileri yer alıyordu.
Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	n February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum

			as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.
Ağustos 2017	Onliner Spambot	Email addresses Passwords	In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.	Ağustos 2017'de, güvenlik araştırmacısı Benkow moɈuƎq tarafından Onliner Spambot adlı bir spam botu tespit edildi. Kötü amaçlı yazılım, Hollanda'daki bir IP adresinde bulunan ve çok sayıda kişisel bilgi içeren dosyayı açığa çıkaran sunucu tabanlı bir bileşen içeriyordu. Toplamda 711 milyon benzersiz e-posta adresi vardı ve bunların çoğuna karşılık gelen şifreler de eşlik ediyordu. Bulunan verilerle ilgili ayrıntılı bilgi, "711 Milyon Kayıtlık Dev Onliner Spambot Dökümünün İç Yüzü" başlıklı blog yazısında yer almaktadır.

Ocak 2017	River City Media Spam List	Email addresses IP addresses Names Physical addresses	In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.	Ocak 2017'de, River City Media'ya ait devasa bir veri yığını internette ifşa edildi. Verilerde, e-posta ve IP adresleri, isimler ve fiziksel adresler de dahil olmak üzere yaklaşık 1,4 milyar kayıt bulunduğu ve bunların tamamının devasa bir spam operasyonunun parçası olarak kullanıldığı tespit edildi. Yinelenen kayıtlar ayıklandıktan sonra, ifşa edilen verilerde 393 milyon benzersiz e-posta adresi olduğu ortaya çıktı.

3- mcavus@ibb.gov.tr – 2 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz

			turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.

4- h.gencdal@ibb.gov.tr – 3 adet Sızıntı - HIBP (haveibeenpwned.com)

Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.
Ağustos 2017	Onliner Spambot	Email addresses Passwords	In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of	Ağustos 2017'de, güvenlik araştırmacısı Benkow moɈuƎq tarafından Onliner Spambot adlı bir spam botu tespit edildi. Kötü amaçlı yazılım, Hollanda'daki bir IP adresinde bulunan ve çok sayıda kişisel bilgi içeren dosyayı açığa çıkaran sunucu tabanlı bir bileşen içeriyordu. Toplamda 711 milyon benzersiz e-posta adresi vardı ve bunların çoğuna karşılık gelen şifreler de eşlik ediyordu. Bulunan verilerle ilgili

			which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.	ayrıntılı bilgi, "711 Milyon Kayıtlık Dev Onliner Spambot Dökümünün İç Yüzü" başlıklı blog yazısında yer almaktadır.
Ocak 2017	River City Media Spam List	Email addresses IP addresses Names Physical addresses	In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.	Ocak 2017'de, River City Media'ya ait devasa bir veri yığını internette ifşa edildi. Verilerde, e-posta ve IP adresleri, isimler ve fiziksel adresler de dahil olmak üzere yaklaşık 1,4 milyar kayıt bulunduğu ve bunların tamamının devasa bir spam operasyonunun parçası olarak kullanıldığı tespit edildi. Yinelenen kayıtlar ayıklandıktan sonra, ifşa edilen verilerde 393 milyon benzersiz e-posta adresi olduğu ortaya çıktı.

5- f.yilmaz@ibb.gov.tr – 4 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Ekim 2019	Data Enrichment Exposure From PDL Customer	Email addresses Employers Geographic locations Job titles Names Phone numbers Social media profiles	In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million	Ekim 2019'da güvenlik araştırmacıları Vinny Troia ve Bob Diachenko, 1,2 milyar kişisel veri kaydı içeren korumasız bir Elasticsearch sunucusu tespit etti. Açığa çıkan veriler arasında, veri zenginleştirme şirketi People Data Labs'ten (PDL) kaynaklandığını gösteren bir indeks ve 622 milyon benzersiz e-posta adresi bulunuyordu. Sunucu PDL'ye ait değildi ve bir müşterinin veritabanını düzgün bir

			unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.	şekilde güvence altına almadığı düşünülüyor. Açığa çıkan bilgiler arasında e-posta adresleri, telefon numaraları, sosyal medya profilleri ve iş geçmişi verileri yer alıyordu.
Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.

Ocak 2017	River City Media Spam List	Email addresses IP addresses Names Physical addresses	In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.	Ocak 2017'de, River City Media'ya ait devasa bir veri yığını internette ifşa edildi. Verilerde, e-posta ve IP adresleri, isimler ve fiziksel adresler de dahil olmak üzere yaklaşık 1,4 milyar kayıt bulunduğu ve bunların tamamının devasa bir spam operasyonunun parçası olarak kullanıldığı tespit edildi. Yinelenen kayıtlar ayıklandıktan sonra, ifşa edilen verilerde 393 milyon benzersiz e-posta adresi olduğu ortaya çıktı.

6- h.zeyveli@ibb.gov.tr – 4 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini

			partnered with HIBP to help victims of cybercrime understand their exposure.	anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.

Ağustos 2017	Onliner Spambot	Email addresses Passwords	In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.	Ağustos 2017'de, güvenlik araştırmacısı Benkow moɈuƎq tarafından Onliner Spambot adlı bir spam botu tespit edildi. Kötü amaçlı yazılım, Hollanda'daki bir IP adresinde bulunan ve çok sayıda kişisel bilgi içeren dosyayı açığa çıkaran sunucu tabanlı bir bileşen içeriyordu. Toplamda 711 milyon benzersiz e-posta adresi vardı ve bunların çoğuna karşılık gelen şifreler de eşlik ediyordu. Bulunan verilerle ilgili ayrıntılı bilgi, "711 Milyon Kayıtlık Dev Onliner Spambot Dökümünün İç Yüzü" başlıklı blog yazısında yer almaktadır.
Ocak 2017	River City Media Spam List	Email addresses IP addresses Names Physical addresses	In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.	Ocak 2017'de, River City Media'ya ait devasa bir veri yığını internette ifşa edildi. Verilerde, e-posta ve IP adresleri, isimler ve fiziksel adresler de dahil olmak üzere yaklaşık 1,4 milyar kayıt bulunduğu ve bunların tamamının devasa bir spam operasyonunun parçası olarak kullanıldığı tespit edildi. Yinelenen kayıtlar ayıklandıktan sonra, ifşa edilen verilerde 393 milyon benzersiz e-posta adresi olduğu ortaya çıktı.

7- nefise.uygun@ibb.gov.tr – 6 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Mayıs 2024	Combolists Posted to Telegram	Email addresses Passwords Usernames	In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data	Mayıs 2024'te, kötü amaçlı Telegram kanallarından 361 milyon benzersiz e-posta adresi içeren 2 milyar satır veri derlendi. Veriler, e-posta adresleri, kullanıcı adları, şifreler ve çoğu durumda bunların girildiği web sitelerini içeren 1.700 dosyada toplam 122 GB boyutundaydı. Verilerin, mevcut kombinasyon listeleri ve bilgi hırsızı kötü amaçlı yazılımların

			appears to have been sourced from a combination of existing combolists and info stealer malware.	bir kombinasyonundan kaynaklandığı anlaşılıyor.
Ocak 2019	Collection #1	Email addresses Passwords	In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.	Ocak 2019'da, popüler bir hacker forumunda dağıtılan büyük bir kimlik bilgisi doldurma listesi (diğer hizmetlerdeki hesapları ele geçirmek için kullanılan e-posta adresleri ve şifre kombinasyonları) keşfedildi. Veriler, 773 milyon benzersiz e-posta adresi ve bu adreslerin diğer ihlal edilmiş hizmetlerde kullandığı şifreler de dahil olmak üzere yaklaşık 2,7 milyar kayıt içeriyordu. Olayla ilgili tüm ayrıntılar ve ihlal edilen şifrelerin nasıl aranacağı, "773 Milyon Kayıtlık 'Koleksiyon #1' Veri İhlali" başlıklı blog yazısında verilmiştir.

Eylül 2018	Kayo.moe Credential Stuffing List	Email addresses Passwords	In September 2018, a collection of almost 42 million email address and plain text password pairs was uploaded to the anonymous file sharing service kayo.moe. The operator of the service contacted HIBP to report the data which, upon further investigation, turned out to be a large credential stuffing list. For more information, read about The 42M Record kayo.moe Credential Stuffing Data.	Eylül 2018'de, yaklaşık 42 milyon e-posta adresi ve düz metin parola çiftinden oluşan bir veri, anonim dosya paylaşım hizmeti kayo.moe'ye yüklendi. Hizmetin operatörü, verileri HIBP'ye bildirdi ve daha sonra yapılan incelemede bunun büyük bir kimlik bilgisi doldurma listesi olduğu ortaya çıktı. Daha fazla bilgi için, "42 Milyonluk Kayıt: kayo.moe Kimlik Bilgisi Doldurma Verileri" başlıklı yazıyı okuyun.
Aralık 2016	Anti Public Combo List	Email addresses Passwords	In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another	Aralık 2016'da, "Anti Public" olarak adlandırılan bir "karma liste"de çok sayıda e-posta adresi ve parola çifti ortaya çıktı. Liste, çoğu çeşitli çevrimiçi sistemlerden ele geçirilmiş birden fazla farklı parolaya sahip 458 milyon benzersiz e-posta adresi içeriyordu. Liste geniş çapta dolaşıma girdi ve "kimlik bilgisi doldurma" için kullanıldı; yani saldırganlar, hesap sahibinin parolasını yeniden kullandığı diğer çevrimiçi sistemleri tespit etme girişiminde bulunmak için bu listeyi kullandılar. Bu olay hakkında ayrıntılı bilgi için, "Have I Been Pwned" kitabındaki "Parola yeniden kullanımı, kimlik bilgisi doldurma ve bir milyar kayıt daha" başlıklı makaleyi okuyun.

			billion records in Have I Been Pwned.	
Ekim 2016	Exploit.In	Email addresses Passwords	In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.	2016 yılının sonlarında, "Exploit.In" olarak adlandırılan bir "birleşik liste"de çok sayıda e-posta adresi ve parola çifti ortaya çıktı. Liste, çoğu çeşitli çevrimiçi sistemlerden ele geçirilmiş birden fazla farklı parolaya sahip 593 milyon benzersiz e-posta adresi içeriyordu. Liste geniş çapta dolaşıma girdi ve "kimlik bilgisi doldurma" için kullanıldı; yani saldırganlar, hesap sahibinin parolasını yeniden kullandığı diğer çevrimiçi sistemleri tespit etme girişiminde bulunmak için bu listeyi kullandılar. Bu olay hakkında ayrıntılı bilgi için, "Have I Been Pwned" kitabındaki "Parola yeniden kullanımı, kimlik bilgisi doldurma ve bir milyar kayıt daha" başlıklı makaleyi okuyun.

8- naile.sen@ibb.gov.tr– 4 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Mayıs 2024	Combolists Posted to Telegram	Email addresses Passwords Usernames	In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data	Mayıs 2024'te, kötü amaçlı Telegram kanallarından 361 milyon benzersiz e-posta adresi içeren 2 milyar satır veri derlendi. Veriler, e-posta adresleri, kullanıcı adları, şifreler ve çoğu durumda bunların girildiği web sitelerini içeren 1.700 dosyada toplam 122 GB boyutundaydı. Verilerin, mevcut kombinasyon listeleri ve bilgi hırsızı kötü amaçlı yazılımların bir

			appears to have been sourced from a combination of existing combolists and info stealer malware.	kombinasyonundan kaynaklandığı anlaşılıyor.
Aralık 2016	Anti Public Combo List	Email addresses Passwords	In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.	Aralık 2016'da, "Anti Public" olarak adlandırılan bir "karma liste"de çok sayıda e-posta adresi ve parola çifti ortaya çıktı. Liste, çoğu çeşitli çevrimiçi sistemlerden ele geçirilmiş birden fazla farklı parolaya sahip 458 milyon benzersiz e-posta adresi içeriyordu. Liste geniş çapta dolaşıma girdi ve "kimlik bilgisi doldurma" için kullanıldı; yani saldırganlar, hesap sahibinin parolasını yeniden kullandığı diğer çevrimiçi sistemleri tespit etme girişiminde bulunmak için bu listeyi kullandılar. Bu olay hakkında ayrıntılı bilgi için, "Have I Been Pwned" kitabındaki "Parola yeniden kullanımı, kimlik bilgisi doldurma ve bir milyar kayıt daha" başlıklı makaleyi okuyun.

Ekim 2016	Exploit.In	Email addresses Passwords	In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.	2016 yılının sonlarında, "Exploit.In" olarak adlandırılan bir "birleşik liste"de çok sayıda e-posta adresi ve parola çifti ortaya çıktı. Liste, çoğu çeşitli çevrimiçi sistemlerden ele geçirilmiş birden fazla farklı parolaya sahip 593 milyon benzersiz e-posta adresi içeriyordu. Liste geniş çapta dolaşıma girdi ve "kimlik bilgisi doldurma" için kullanıldı; yani saldırganlar, hesap sahibinin parolasını yeniden kullandığı diğer çevrimiçi sistemleri tespit etme girişiminde bulunmak için bu listeyi kullandılar. Bu olay hakkında ayrıntılı bilgi için, "Have I Been Pwned" kitabındaki "Parola yeniden kullanımı, kimlik bilgisi doldurma ve bir milyar kayıt daha" başlıklı makaleyi okuyun.

9- saliha.peru@ibb.gov.tr – 4 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Ocak 2021	Twitter (200M)	Email addresses Names Social media profiles Usernames	In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email	2023 yılının başlarında, Twitter'dan elde edilen 200 milyondan fazla kayıt popüler bir siber saldırı forumunda ortaya çıktı. Veriler, 2021 yılında e-posta adreslerinin Twitter profillerine çözümlenmesini sağlayan bir API'nin kötüye kullanılmasıyla elde edilmişti. Elde edilen sonuçlar daha sonra e-posta adreslerinin yanı sıra isimler, kullanıcı adları ve takipçi sayıları da dahil olmak

			addresses alongside public Twitter profile information including names, usernames and follower counts.	üzere herkese açık Twitter profil bilgilerini içeren bir veri kümesi haline getirildi.
Ekim 2017	MyHeritage	Email addresses Passwords	In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly.	Ekim 2017'de, soy ağacı sitesi MyHeritage bir veri ihlaline uğradı. Olay, bir güvenlik araştırmacısının verileri keşfetmesi ve MyHeritage ile iletişime geçmesinden 7 ay sonra bildirildi. Toplamda, 92 milyondan fazla müşteri kaydı ifşa edildi ve bunlar arasında e-posta adresleri ve tuzlanmış SHA-1 parola özetleri yer alıyordu. 2019'da, veriler (diğer birçok büyük ihlal ile birlikte) karanlık web pazarında satışa sunulmuş olarak ortaya çıktı ve daha sonra daha geniş çapta yayılmaya başladı.
Ekim 2016	Dailymotion	Email addresses Passwords Usernames	In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames	Ekim 2016'da video paylaşım platformu Dailymotion bir veri ihlaline uğradı. Saldırı, 85 milyondan fazla kullanıcı hesabının ifşa olmasına yol açtı ve e-posta adresleri, kullanıcı adları ve parolaların bcrypt özetlerini içeriyordu.

			and bcrypt hashes of passwords.	

10- hsan@ibb.gov.tr – 3 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.

Kasım 2020	Cit0day	Email addresses Passwords	In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.	Kasım 2020'de, Cit0day olarak bilinen ve 23.000'den fazla ihlal edildiği iddia edilen web sitesinden oluşan bir veri koleksiyonu, çeşitli hacker forumlarında indirilmeye sunuldu. Veriler, genellikle hem parola karmaları hem de kırılmış, düz metin sürümleri olarak sunulan parola çiftleriyle birlikte 226 milyon benzersiz e-posta adresinden oluşuyordu. Verilerin bağımsız olarak doğrulanması, daha önce açıklanmamış birçok meşru ihlal içerdiğini ortaya koydu. Veriler, dehashed.com tarafından HIBP'ye sağlandı.
Ocak 2019	Collection #1	Email addresses Passwords	In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.	Ocak 2019'da, popüler bir hacker forumunda dağıtılan büyük bir kimlik bilgisi doldurma listesi (diğer hizmetlerdeki hesapları ele geçirmek için kullanılan e-posta adresleri ve şifre kombinasyonları) keşfedildi. Veriler, 773 milyon benzersiz e-posta adresi ve bu adreslerin diğer ihlal edilmiş hizmetlerde kullandığı şifreler de dahil olmak üzere yaklaşık 2,7 milyar kayıt içeriyordu. Olayla ilgili tüm ayrıntılar ve ihlal edilen şifrelerin nasıl aranacağı, "773 Milyon Kayıtlık 'Koleksiyon #1' Veri İhlali" başlıklı blog yazısında verilmiştir.

11- beyazmasa@ibb.gov.tr – 7 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Şubat 2020	Covve	Email addresses Job titles Names Phone numbers Physical addresses Social media profiles	In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between	Şubat 2020'de, "db8151dd" olarak adlandırılan devasa bir kişisel bilgi yığını, herkese açık bir Elasticsearch sunucusunda açıkta bırakılmış halde bulunduktan sonra HIBP'ye sağlandı. Daha sonra Covve kişiler uygulaması kaynaklı olduğu belirlenen veriler, Covve kullanıcıları ve kişileri arasındaki kapsamlı kişisel bilgileri ve etkileşimleri içeriyordu. Veriler, dehashed.com tarafından HIBP'ye sağlandı.

			Covve users and their contacts. The data was provided to HIBP by dehashed.com.	
Ekim 2019	Data Enrichment Exposure From PDL Customer	Email addresses Employers Geographic locations Job titles Names Phone numbers Social media profiles	In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.	Ekim 2019'da güvenlik araştırmacıları Vinny Troia ve Bob Diachenko, 1,2 milyar kişisel veri kaydı içeren korumasız bir Elasticsearch sunucusu tespit etti. Açığa çıkan veriler arasında, veri zenginleştirme şirketi People Data Labs'ten (PDL) kaynaklandığını gösteren bir indeks ve 622 milyon benzersiz e-posta adresi bulunuyordu. Sunucu PDL'ye ait değildi ve bir müşterinin veritabanını düzgün bir şekilde güvence altına almadığı düşünülüyor. Açığa çıkan bilgiler arasında e-posta adresleri, telefon numaraları, sosyal medya profilleri ve iş geçmişi verileri yer alıyordu.

Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.

Temmuz 2018	Apollo	Email addresses Employers Geographic locations Job titles Names Phone numbers Salutations Social media profiles	In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.	Temmuz 2018'de, satış etkileşimi girişimi Apollo, milyarlarca veri noktası içeren bir veritabanını şifresiz olarak herkese açık bir şekilde bıraktı. Veriler, güvenlik araştırmacısı Vinny Troia tarafından keşfedildi ve Troia daha sonra 126 milyon benzersiz e-posta adresini içeren verilerin bir alt kümesini Have I Been Pwned'e gönderdi. Apollo tarafından açıkta bırakılan veriler, "gelir hızlandırma platformunda" kullanılıyordu ve isimler ve e-posta adresleri gibi kişisel bilgilerin yanı sıra iş yerleri, pozisyonlar ve bulundukları yer gibi mesleki bilgileri de içeriyordu. Apollo, açıkta bırakılan verilerin şifreler, sosyal güvenlik numaraları veya finansal veriler gibi hassas bilgiler içermediğini vurguladı. Apollo web sitesinde, kuruluşla iletişime geçmek isteyenler için bir iletişim formu bulunmaktadır.

Ağustos 2017	Onliner Spambot	Email addresses Passwords	In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.	Ağustos 2017'de, güvenlik araştırmacısı Benkow moɈuƎq tarafından Onliner Spambot adlı bir spam botu tespit edildi. Kötü amaçlı yazılım, Hollanda'daki bir IP adresinde bulunan ve çok sayıda kişisel bilgi içeren dosyayı açığa çıkaran sunucu tabanlı bir bileşen içeriyordu. Toplamda 711 milyon benzersiz e-posta adresi vardı ve bunların çoğuna karşılık gelen şifreler de eşlik ediyordu. Bulunan verilerle ilgili ayrıntılı bilgi, "711 Milyon Kayıtlık Dev Onliner Spambot Dökümünün İç Yüzü" başlıklı blog yazısında yer almaktadır.
Temmuz 2016	AKP Emails	Email addresses Email messages	In July 2016, a hacker known as Phineas Fisher hacked Turkey's ruling party (Justice and Development Party or "AKP") and gained access to 300k emails. The full contents of the emails were subsequently published by WikiLeaks and made searchable. HIBP identified over 917k unique email address patterns in the data set, including message IDs and a number of other non-user addresses.	Temmuz 2016'da Phineas Fisher olarak bilinen bir hacker, Türkiye'nin iktidardaki partisi (Adalet ve Kalkınma Partisi veya "AKP")'nin sistemini hackleyerek 300 bin e-postaya erişim sağladı. E-postaların tüm içeriği daha sonra WikiLeaks tarafından yayınlandı ve aranabilir hale getirildi. HIBP, veri setinde mesaj kimlikleri ve bir dizi diğer kullanıcı dışı adres de dahil olmak üzere 917 binden fazla benzersiz e-posta adresi kalıbı tespit etti.

12- bozkul@ibb.gov.tr – 4 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.

Ekim 2019	Data Enrichment Exposure From PDL Customer	Email addresses Employers Geographic locations Job titles Names Phone numbers Social media profiles	In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.	Ekim 2019'da güvenlik araştırmacıları Vinny Troia ve Bob Diachenko, 1,2 milyar kişisel veri kaydı içeren korumasız bir Elasticsearch sunucusu tespit etti. Açığa çıkan veriler arasında, veri zenginleştirme şirketi People Data Labs'ten (PDL) kaynaklandığını gösteren bir indeks ve 622 milyon benzersiz e-posta adresi bulunuyordu. Sunucu PDL'ye ait değildi ve bir müşterinin veritabanını düzgün bir şekilde güvence altına almadığı düşünülüyor. Açığa çıkan bilgiler arasında e-posta adresleri, telefon numaraları, sosyal medya profilleri ve iş geçmişi verileri yer alıyordu.
Şubat 2019	Verifications.io	Dates of birth Email addresses Employers Genders Geographic locations IP addresses Job titles Names Phone numbers Physical addresses	In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the	Şubat 2019'da, e-posta adresi doğrulama hizmeti verifications.io bir veri ihlaline uğradı. Bob Diachenko ve Vinny Troia tarafından keşfedilen ihlal, verilerin şifresiz olarak herkese açık bırakılan bir MongoDB örneğinde saklanmasından kaynaklanıyordu ve 763 milyon benzersiz e-posta adresinin ifşa edilmesine yol açtı. Verilerdeki birçok kayıt ayrıca adlar, telefon numaraları, IP adresleri, doğum tarihleri ve cinsiyetler

			data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.	gibi ek kişisel bilgiler de içeriyordu. Verilerde şifre bulunmuyordu. Verifications.io web sitesi, ifşa süreci boyunca çevrimdışı kaldı, ancak arşivlenmiş bir kopyası hala görüntülenebilir durumda.
Ocak 2017	River City Media Spam List	Email addresses IP addresses Names Physical addresses	In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.	Ocak 2017'de, River City Media'ya ait devasa bir veri yığını internette ifşa edildi. Verilerde, e-posta ve IP adresleri, isimler ve fiziksel adresler de dahil olmak üzere yaklaşık 1,4 milyar kayıt bulunduğu ve bunların tamamının devasa bir spam operasyonunun parçası olarak kullanıldığı tespit edildi. Yinelenen kayıtlar ayıklandıktan sonra, ifşa edilen verilerde 393 milyon benzersiz e-posta adresi olduğu ortaya çıktı.

13- alpergo@ibb.gov.tr – 1 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure.	2025 yılında, tehdit istihbaratı firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyordu. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.

14- burhanayan@ibb.gov.tr – 0 adet Sızıntı - HIBP (haveibeenpwned.com)

SIZINTI TESPİT EDİLMEMİŞTİR.

15-ikizzeynep.mutlu@ibb.gov.tr – 1 adet Sızıntı - HIBP(haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure	2025 yılında, siber tehdit istihbarat firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyor. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.

16- adilyildirim@ibb.gov.tr – 3 adet Sızıntı - HIBP (haveibeenpwned.com)

Nisan 2025	Synthient Credential Stuffing Threat Data	Email addresses Passwords	During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across multiple malicious internet sources. Comprised of email addresses and passwords from previous data breaches, these lists are used by attackers to compromise other, unrelated accounts of victims who have reused their passwords. The data also included 1.3 billion unique passwords, which are now searchable in Pwned Passwords. Working to turn breached data into awareness, Synthient partnered with HIBP to help victims of cybercrime understand their exposure	2025 yılında, siber tehdit istihbarat firması Synthient, çeşitli kötü amaçlı internet kaynaklarında bulunan kimlik bilgilerini ele geçirme listelerinde açıklanan 2 milyar benzersiz e-posta adresini bir araya getirdi. Önceki veri ihlallerinden elde edilen e-posta adresleri ve şifrelerden oluşan bu listeler, saldırganlar tarafından kurbanların şifrelerini tekrar kullandıkları diğer, ilgisiz hesaplarını ele geçirmek için kullanılıyor. Veriler ayrıca, artık Pwned Passwords'da aranabilir olan 1,3 milyar benzersiz şifreyi de içeriyor. İhlal edilen verileri farkındalığa dönüştürmek için çalışan Synthient, siber suç mağdurlarının risklerini anlamalarına yardımcı olmak amacıyla HIBP ile ortaklık kurdu.
Şubat 2025	ALIEN TXTBASE Stealer Logs	Email addresses Passwords	In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website.	Şubat 2025'te, ALIEN TXTBASE olarak bilinen bir Telegram kanalından 23 milyar satırlık hırsızlık günlüğü elde edildi. Veriler, 284 milyon benzersiz e-posta adresinin yanı sıra bu adreslerin girildiği web sitelerini ve kullanılan şifreleri içeriyordu. Bu veriler artık HIBP'de hem e-posta alan adı hem de hedef web sitesinin alan adı ile aranabilir durumda.

Mayıs 2024	Combolists Posted to Telegram	Email addresses Passwords Usernames	In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.	Mayıs 2024'te, kötü amaçlı Telegram kanallarından 361 milyon benzersiz e-posta adresi içeren 2 milyar satır veri derlendi. Veriler, e-posta adresleri, kullanıcı adları, şifreler ve çoğu durumda bunların girildiği web sitelerini içeren 1.700 dosyada toplam 122 GB boyutundaydı. Verilerin, mevcut kombinasyon listeleri ve bilgi hırsızı kötü amaçlı yazılımların bir kombinasyonundan kaynaklandığı anlaşılıyor.

17- ibasaran@ibb.gov.tr – 3 adet Sızıntı - HIBP (haveibeenpwned.com)

Aralık 2016	Anti Public Combo List	Email addresses Passwords	In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.	Aralık 2016'da, "Anti Public" olarak adlandırılan bir "karma liste"de çok sayıda e-posta adresi ve parola çifti ortaya çıktı. Liste, çoğu çeşitli çevrimiçi sistemlerden ele geçirilmiş birden fazla farklı parolaya sahip 458 milyon benzersiz e-posta adresi içeriyordu. Liste geniş çapta dolaşıma girdi ve "kimlik bilgisi doldurma" için kullanıldı; yani saldırganlar, hesap sahibinin parolasını yeniden kullandığı diğer çevrimiçi sistemleri tespit etme girişiminde bulunmak için bu listeyi kullandılar. Bu olay hakkında ayrıntılı bilgi için, "Have I Been Pwned" kitabındaki "Parola yeniden kullanımı, kimlik bilgisi doldurma ve bir milyar kayıt daha" başlıklı makaleyi okuyun.

Ekim 2016	Exploit.In	Email addresses Passwords	In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.	2016 yılının sonlarında, "Exploit.In" olarak adlandırılan bir "birleşik liste"de çok sayıda e-posta adresi ve parola çifti ortaya çıktı. Liste, çoğu çeşitli çevrimiçi sistemlerden ele geçirilmiş birden fazla farklı parolaya sahip 593 milyon benzersiz e-posta adresi içeriyordu. Liste geniş çapta dolaşıma girdi ve "kimlik bilgisi doldurma" için kullanıldı; yani saldırganlar, hesap sahibinin parolasını yeniden kullandığı diğer çevrimiçi sistemleri tespit etme girişiminde bulunmak için bu listeyi kullandılar. Bu olay hakkında ayrıntılı bilgi için, "Have I Been Pwned" kitabındaki "Parola yeniden kullanımı, kimlik bilgisi doldurma ve bir milyar kayıt daha" başlıklı makaleyi okuyun.
Temmuz 2008	MySpace	Email addresses Passwords Usernames	In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.	Yaklaşık 2008 yılında MySpace, yaklaşık 360 milyon hesabı açığa çıkaran bir veri ihlali yaşadı. Mayıs 2016'da veriler, "Real Deal" adlı karanlık pazar web sitesinde satışa sunuldu ve e-posta adresleri, kullanıcı adları ve parolaların ilk 10 karakterinin küçük harfe dönüştürülmüş ve tuzlama yapılmadan saklanmış SHA1 özetlerini içeriyordu. İhlalin kesin tarihi bilinmiyor, ancak verilerin analizi, kamuoyuna açıklanmasından 8 yıl önce gerçekleştiğini gösteriyor.

BİLİRKİŞİ RAPORU
BÖLÜM – 3
SONUÇ

1- İddianamede atılı suç kapsamında ele geçirildiği iddia edilen veriler ile ilgili olarak *bahsi geçen verilerin ibb.gov.tr veri tabanından ele geçirilip geçirilmediği,

İddianamedeki yazı/yetkilendirme net şekilde okunmamaktadır. İlgili yazı internette örneği araştırılarak tespit edilmiş olup,

*"Belediyemiz Müfettişlerinden Emine Sema Ballı ve Kaya Albayrak Belediyemiz çalışanlarından ve/veya dışarıdan belirlenecek üç uzman ile Belediyemiz ve Bağlı kuruluşlarının elektronik veri tabanı ve altyapılarında her türlü inceleme ve araştırmayı yapmaya ve veri tabanı ve altyapıyı kopyalamaya yetkilendirilmiştir."*denilmektedir.

Kaynak: https://www.haberturk.com/ekrem-imamoglundan-belediyenin-tum-veri-tabanini-kopyalatma-talimati-2436976?page=3

İlgili yazıya istinaden altyapı/altyapılara ve veri tabanı/veri tabanlarına ilişkin görevlendirme olduğu anlaşılmakla ancak yapılan iş ve işlemlerin ne olduğuna ilişkin tutanak, bilgi ya da belge olmadığından herhangi bir değerlendirme yapmak mümkün olamayacaktır.

2- Anılan veri tabanından ele geçirildi ise ne şekilde (hackleme/sızma) hangi tarihte ele geçirildiği,

İş bu raporun **BÖLÜM-3 SONUÇ** bölümünün **birinci maddesinde** izah edildiği üzere herhangi bir değerlendirme yapmak mümkün olamayacaktır.

3- *İddianame anlatımında geçen OSINT ve DARKWEB ifadeleri gözetildiğinde bu verilerin atılı suç tarihi öncesinde internet ortamına sızmış veriler olup, olmadığı,

Verilerin atılı suç tarihi öncesinde internet ortamına sızmış veriler olup, olmadığı net bir şekilde tespit edilemeyeceği iş bu raporun **BÖLÜM-1, F- VERİ SIZINTISI (DATA LEAK / DATA BREACH) bölümündeki "Profesyonel/Uzman tehdit aktörlerinin genel yaklaşımı;"** alanında ifade edildiği üzere teknik olarak tam net tarih belirlenmesi mümkün olamayacaktır. İş bu raporun **BÖLÜM-1, G-DARKNET VE DARK WEB KAVRAMLARI, H-DARK WEB İÇERİK EKOSİSTEMİ, İ- OSINT * AÇIK KAYNAK İSTİHBARATI (OPEN SOURCE INTELLİGENCE – OSINT)** maddelerinde ve iş bu raporun **BÖLÜM-2 TEKNİK ANALİZ** kısmında izah edildiği üzere internete sızmış veriler içerisinde kullanıcı bilgileri tespit edilebilmektedir. Takdiri Sayın Mahkeme Heyeti'nize aittir.

4- Sızdı ise bu verilerin hangi tarihte ne şekilde internet ortamına sızdığı,

İş bu raporun **BÖLÜM-2 TEKNİK ANALİZ** bölümünde incelendiği üzere internete sızmış veriler içerisinde kullanıcı bilgileri tespit edilebilmektedir. İlgili özet tablo aşağıdaki gibidir.

No	Kullanıcı/Eposta	Sızıntı Adedi HIBP	Sızıntı Tarihi HIBP	Sızıntı Tanımı HIBP	Sızıntı Adedi DataBreach	Sızıntı Tarihi DataBreach	Sızıntı Tanımı DataBreach	Sızıntı Adedi DeHashed	Sızıntı Tanımı DeHashed	Sızıntı Tarihi DeHashed
1	isfalt@ibb.gov.tr	4	Nisan 2025 Ekim 2019 Şubat 2019 Ocak 2017	Synthient Credential Stuffing Threat Data Data Enrichment Exposure From PDL Customer Verifications.io River City Media Spam List	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	1	Collections	Bilgi Yok
2	h.karakaya@ibb.gov.tr	5	Nisan 2025 Ekim 2019 Şubat 2019 Ağustos 2017 Ocak 2017	Synthient Credential Stuffing Threat Data Data Enrichment Exposure From PDL Customer Verifications.io Onliner Spambot River City Media Spam List	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	1	Collections	Bilgi Yok
3	mcavus@ibb.gov.tr	2	Nisan 2025 Şubat 2019	Synthient Credential Stuffing Threat Data Verifications.io	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	1	Collections	Bilgi Yok
4	h.gencdal@ibb.gov.tr	3	Şubat 2019 Ağustos 2017 Ocak 2017	Verifications.io Onliner Spambot River City Media Spam List	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	1	Collections	Bilgi Yok
5	f.yilmaz@ibb.gov.tr	4	Nisan 2025 Ekim 2019 Şubat 2019 Ocak 2017	Synthient Credential Stuffing Threat Data Data Enrichment Exposure From PDL Customer Verifications.io River City Media Spam List	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	1	Collections	Bilgi Yok
6	h.zeyveli@ibb.gov.tr	4	Nisan 2025 Şubat 2019 Ağustos 2017 Ocak 2017	Synthient Credential Stuffing Threat Data Verifications.io Onliner Spambot River City Media Spam List	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	1	Collections	Bilgi Yok
7	nefise.uygun@ibb.gov.tr	6	Nisan 2025 Mayıs 2024 Ocak 2019 Eylül 2018 Aralık 2016 Ekim 2016	Synthient Credential Stuffing Threat Data Combolists Posted to Telegram Collection #1 Kayo.moe Credential Stuffing List Anti Public Combo List Exploit.In	4	7 Ocak 2019 16 Aralık 2016 13 Ekim 2016 1 Ocak 2014	Collection #1-5 Anti Public Exploit.in Ubisoft Forum	4	Exploit.in Exploit.in Collections AntiPublic	Bilgi Yok
8	naile.sen@ibb.gov.tr	4	Nisan 2025 Mayıs 2024 Aralık 2016 Ekim 2016	Synthient Credential Stuffing Threat Data Combolists Posted to Telegram Anti Public Combo List Exploit.In	3	7 Ocak 2019 16 Aralık 2016 13 Ekim 2016	Collection #1-5 Anti Public Exploit.in	1	AntiPublic	Bilgi Yok
9	saliha.peru@ibb.gov.tr	4	Nisan 2025 Ocak 2021 Ekim 2017 Ekim 2016	Synthient Credential Stuffing Threat Data Twitter (200M) MyHeritage Dailymotion	5	2 Nisan 2025 1 Ocak 2021 7 Ocak 2019 26 Ekim 2017 20 Ekim 2016	X (Twitter) Twitter Collection #1-5 MyHeritage Dailymotion	3	MyHeritage.com Twitter.com Dailymotion	Bilgi Yok
10	hsan@ibb.gov.tr	3	Nisan 2025 Kasım 2020 Ocak 2019	Synthient Credential Stuffing Threat Data Cit0day Collection #1	2	4 Kasım 2020 7 Ocak 2019	Cit0day Collection #1-5	2	Collections Collections	Bilgi Yok
11	beyazmasa@ibb.gov.tr	7	Nisan 2025 Şubat 2020 Ekim 2019 Şubat 2019 Temmuz 2018 Ağustos 2017 Temmuz 2016	Synthient Credential Stuffing Threat Data Covve Data Enrichment Exposure From PDL Customer Verifications.io Apollo Onliner Spambot AKP Emails	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	0	Sızıntı Bilgisi Yok	Bilgi Yok
12	bozkul@ibb.gov.tr	4	Nisan 2025 Ekim 2019 Şubat 2019 Ocak 2017	Synthient Credential Stuffing Threat Data Data Enrichment Exposure From PDL Customer Verifications.io River City Media Spam List	2	25 Şubat 2019 7 Ocak 2019	Verifications.io Collection#1-5	0	Sızıntı Bilgisi Yok	Bilgi Yok
13	alpergo@ibb.gov.tr	1	Nisan 2025	Synthient Credential Stuffing Threat Data	1	7 Ocak 2019	Collection#1-5	0	Sızıntı Bilgisi Yok	Bilgi Yok
14	burhanayan@ibb.gov.tr	0	Bilgi Yok	Sızıntı Bilgisi Yok	1	7 Ocak 2019	Collection#1-5	0	Sızıntı Bilgisi Yok	Bilgi Yok
15	ikizzeynep.mutlu@ibb.gov.tr	1	Nisan 2025	Synthient Credential Stuffing Threat Data	1	7 Ocak 2019	Collection#1-5	0	Sızıntı Bilgisi Yok	Bilgi Yok
16	adilyildirim@ibb.gov.tr	3	Nisan 2025 Şubat 2025 Mayıs 2024	Synthient Credential Stuffing Threat Data ALIEN TXTBASE Stealer Logs Combolists Posted to Telegram	1	7 Ocak 2019	Collection#1-5	0	Sızıntı Bilgisi Yok	Bilgi Yok
17	ibasaran@ibb.gov.tr	3	Aralık 2016 Ekim 2016 Temmuz 2008	Anti Public Combo List Exploit.In Temmuz 2008	4	7 Ocak 2019 16 Aralık 2016 13 Ekim 2016 1 Temmuz 2008	Collection#1-5 Anti Public Exploit.in MySpace	2	AntiPublic Myspace.com	Bilgi Yok

5- Bu verilerin internetin kamuya açık alanlarında bulunup bulunmadığı hususlarında inceleme yapıp,

Görevlendirme kapsamında yapılan teknik araştırma sonucunda, incelemeye konu verilerin veri ihlali indeksleme ve bildirim platformları olan Have I Been Pwned (HIBP) sistemlerinde bulunduğu ve haber içeriklerinin bulunduğu, DeHashed sistemlerinde yer aldığı; ayrıca DataBreaches.net platformunda ilgili ihlale ilişkin kayıtların olduğu tespit edilmiştir.

Bu platformlar, kamuya yansıyan veya sızdırılmış veri setlerini indeksleyen sistemler olup, yapılan tespit söz konusu verilerin daha önce gerçekleşmiş veri ihlalleri kapsamında internete yansımış olabileceğini göstermektedir.

Takdiri Sayın Mahkeme Heyeti'nize ait olmak bilirkişi raporumu saygılarımla sunarım.02/03/2026

E-İMZALIDIR.

Dr. Öğr. Üyesi İsmail Sinan TATLIGİL
Bilirkişi- 10812
Ph.D. Bilgisayar Mühendisliği
M.Sc. Siber Güvenlik
M.Sc. Adli Bilişim Mühendisliği